Sachar Paulus
Norbert Pohlmann
Helmut Reimer

Securing Electronic Business Processes

Highlights of the Information Security Solutions Europe 2004 Conference

Preface

The Information Security Solutions Europe Conference (ISSE) was started in 1999 by EEMA and TeleTrusT with the support of the European Commission and the German Federal Ministry of Technology and Economics. Today the annual conference is a fixed event in every IT security professional's calendar. The aim of ISSE is to support the development of a European information security culture and especially a cross-border framework for trustworthy IT applications for citizens, industry and administration. Therefore, it is important to take into consideration both international developments and European regulations and to allow for the interdisciplinary character of the information security field. In the five years of its existence ISSE has thus helped shape the profile of this specialist area.

The integration of security in IT applications was initially driven only by the actual security issues considered important by experts in the field; currently, however, the economic aspects of the corresponding solutions are the most important factor in deciding their success. ISSE offers a suitable podium for the discussion of the relationship between these considerations and for the presentation of the practical implementation of concepts with their technical, organisational and economic parameters.

An international programme committee is responsible for the selection of the conference contributions and the composition of the programme:

- Jan Bartelen, ABN AMRO (The Netherlands)
- Ronny Bjones, Microsoft (Belgium)
- Alfred Buellesbach, DaimlerChrysler (Germany)
- Lucas Cardholm, Ernst&Young (Sweden)
- Roger Dean, EEMA (UK)
- Marijke De Soete (Belgium)
- Jos Dumortier, KU Leuven (Belgium)
- Loup Gronier, XP conseil (France)
- John Hermans, KPMG (The Netherlands)
- Frank Jorissen, Silicomp Belgium (United Kingdom)
- Jeremy Hilton, EEMA (United Kingdom)
- Matt Landrock, Cryptomathic (Denmark)
- Karel Neuwirt, The Office for Personal Data Protection (Czech Republic)
- Sachar Paulus, SAP (Germany)
- Norbert Pohlmann, TeleTrusT (Germany)
- Reinhard Posch, TU Graz, (Austria)
- Bart Preneel, KU Leuven (Belgium)
- Helmut Reimer, TeleTrusT (Germany)
- Paolo Rossini, TELSY, Telecom Italia Group (Italy)
- Ulrich Sandl, BMWA (Germany)
- Wolfgang Schneider, GMD (Germany)
- Robert Temple, BT (United Kingdom)

Many of the presentations at the conference are of use as reference material for the future, hence this publication. The contributions are based on the presentations of the authors and thus not only document the key issues of the conference but make this information accessible for further interested parties.

The editors have endeavoured to allocate the contributions in these proceedings – which differ from the structure of the conference programme – to topic areas which cover the interests of the readers.

Sachar Paulus *Norbert Pohlmann* *Helmut Reimer*

EEMA (www.eema.org):

For 16 years, EEMA has been Europe's leading independent, non-profit e-Business association, working with its European members, governmental bodies, standards organisations and e-Business initiatives throughout Europe to further e-Business technology and legislation.

EEMA's remit is to educate and inform around 200 Member organisations on the latest developments and technologies, at the same time enabling Members of the association to compare views and ideas. The work produced by the association with its Members (projects, papers, seminars, tutorials and re-ports etc) is funded by both membership subscriptions and revenue generated through fee-paying events. All of the information generated by EEMA and its Members is available to other members free of charge.

Examples of papers produced in recent months are:- Role Based Access Control – a User's Guide, Wireless Deployment Guidelines, Secure e-Mail within the Organisation, The impact of XML on existing Business Processes, PKI Usage within User Organisations. EEMA Members, based on a requirement from the rest of the Membership, contributed all of these papers. Some are the result of many months' work, and form part of a larger project on the subject.

TeleTrusT (www.teletrust.de):

TeleTrusT was founded in 1989 to promote the security of information and communication technology in an open systems environment.

The non-profit organization was constituted with the aim of:

- achieving acceptance of the digital signature as an instrument conferring legal validity on electronic transactions;
- supporting research into methods of safeguarding electronic data interchange (EDI), application of its results, and development of standards in this field;
- collaborating with institutes and organizations in other countries with the aim of harmonizing objectives and standards within the European Union.

TeleTrusT supports the incorporation of trusted services in planned or existing IT applications of public administration, organisations and industry. Special attention is being paid to secure services and their management for trustworthy electronic communication.

Table of Contents

Technology 87

Application 177

Strategy

True Economics of a Security Infrastructure

Andrew Oldham

ASPACE Solutions, Three Tuns House,
109 Borough High Street, London, SE1 1NL, UK
aoldham@aspacesolutions.com

Abstract

Fundamental to a discussion on the financial implications of implementing and running a security infrastructure is that an Identification & Verification (ID&V) solution will not make you money directly. Rather, ID&V is considered to be an enabling technology helping organisations improve operational processes and customer experiences as well as reducing exposure to risk and fraud.
When talking about Return on Investment (ROI) in the context of security, it is important to look to the tangible benefits derived from implementing a security infrastructure – the application of the solution, not the solution itself, can reduce costs and lead to increased revenue.
Due to the multi-channel nature of the financial services sector and the importance of identification and verification in undertaking financial transactions, examples included in this paper are primarily drawn from this market.

1 The cost elements

Organisations seeking to secure their customer communities are only too aware of the need to keep pace with customer demands, industry trends and technological advances.

Implementing, maintaining and using a strong security infrastructure is a costly exercise. Generally speaking, the more complex the solution, the more difficult it is to use and the greater the operating costs.

Quantifying costs versus benefits associated with introduction of security services is an abstract process, predominantly because of the intangible nature of these services.

Deciding upon the measurement criteria to build a business case for a security solution is a difficult process, often based on opinion and speculation. This approach is not dissimilar to the calculations required for BASEL-II; quantification of risk for example, is a notoriously subjective area.

Security solutions are normally implemented for a specific reason; namely to protect a valuable resource. The nature of the resource drives the scale, scope and complexity of the underlying security solution such as the manner in which it is accessed and which user communities are permitted access to it. If solution requires many different types of resources to be secured then the underlying security model becomes even more complex.

S. Paulus, N. Pohlmann, H. Reimer (Editors**):** Securing Electronic Business Processes, Vieweg (2004), 3-11

Figure 1: Cost elements of a security service.

This paper considers the tangible costs associated with the implementation and operation of ID&V services in their support of business processes. It also investigates approaches to cost reduction and identifies the intangible benefits of deploying an enterprise-wide security solution.

The cost elements of a security solution can be considered as the:

- Registration Costs – Registration of users for the security service;
- Servicing Costs – Application of security controls (identification, verification, authorisation);
- Administration Costs – Administration of registered users;
- Operational Costs – Installation and maintenance of the solution.

1.1 Registration costs

A registration process can be described as the sequence of steps required in order to provision a new user. Registration processes are typically supported by a workflow or CRM application, which serves to sequence the steps and invoke appropriate activities. In the retail financial services world, the registration process is analogous to the account opening process. For example, a new-to-brand customer will be led through a series of steps before completing a product application. Certain steps invoke a series of identification processes, such as proof of address or verification of credit worthiness – in the UK financial services sector these are termed Know Your Customer (KYC) checks. Successful completion of these checks results in the provision of a valid user identity and the establishment of trust between the customer and the organisation.

Typically, these security components will include:

- Provision of a unique identifier;
- Provision of one or more verifiers (such as passwords, PIN’s or memorable facts);
- Fulfilment of a physical token (if a strong authentication mechanism is required);
- Provision of a security profile (defining privileges, roles, entitlements and restrictions);
- Enablement of one or more access channels (such as web, branch, interactive voice response (IVR) and phone)

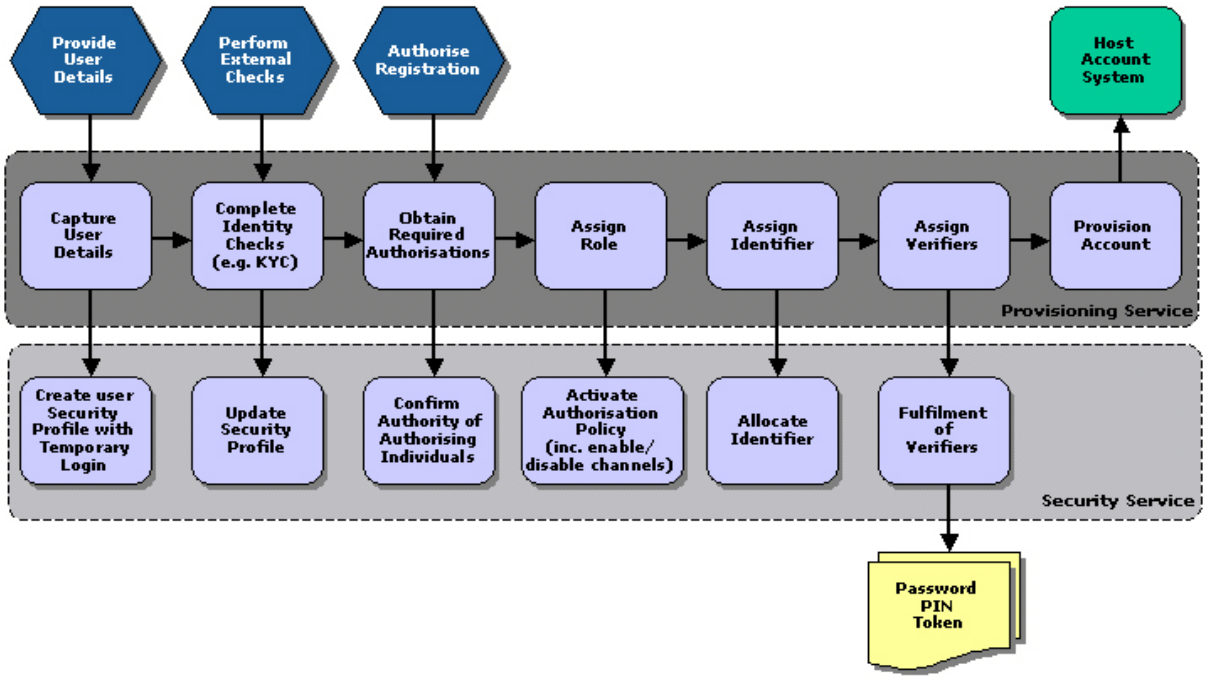

Figure 2: Generic user registration process.

Typically, organisations employ different registration processes and systems for each channel and product, thus duplicating customer interactions, systems and resources.

1.2 Servicing costs

The security components associated with the servicing of a resource relate to the way in which the acts of identification, authentication and authorisation are applied including auditing all activities.

Users access resources either directly through self-service channels (such as the web or IVR) or indirectly through facilitated channels (such as over the phone to contact centres or through branches).

1.2.1 User self-service

In order to reduce operating costs, organisations provide their customers with tools that allow them to service their own resources directly, reducing the number of service agents required.

As the transaction value becomes higher, so the financial risk increases and thus the security controls applied become stronger. Channel access must also be considered, with direct channels, such as web, perceived to be of higher risk than facilitated channels. Therefore, an organisation permitting higher risk transactions, such as a bank transfer, may require the deployment of strong verification mechanisms, for example two-factor authentication or one-time passwords.

Types of security controls applied to user self-service are typically:

- Username and password for authentication;
- Memorable facts as a back-up process for resetting verifiers;
- A second token, such as a smartcard or one time password token for secondary authentication.

Often, there are a number of different underlying security services, which support each direct channel independently, leading to a duplication of functionality (such as use of memorable data, the application of transaction limits).

The associated security costs of enabling self-service are therefore defined by the:

- Types of authentication mechanisms adopted;
- Complexity of security features applied;
- Number of security services implemented.

1.2.2 Facilitated channels

Allowing users to interact with an organisation through facilitated channels should be undertaken with the same security considerations as those for self-service. The security processes adopted must be strong enough to reduce the risk of fraudulent activity, but should be applicable to the situation. For example, it doesn't make sense to use a £10 smartcard to secure a £5 resource.

In facilitated channels, the fact that staff transact upon a resource on behalf of a user means that the audit must record not only what activity was performed, but also which staff member carried out the transaction on behalf of the user. Typically, security solutions supporting facilitated channels are geared up to record activities performed by *either* staff *or* end-users but not both.

When users call a contact centre in order access resources, they are initially identified and authenticated by the service agent. If the service query requires a hand-off to another agent, often it is not possible to transfer the authenticated user session thus requiring the user to re-authenticate. Ideally, an organisation would maintain a consistent audit record of all interactions with the user, such that it is possible to trace the initial authentication by the first agent and then subsequently transfer an authenticated user to a second agent.

The ability to perform an authenticated session transfer reduces the average call time, since a second agent does not need to re-verify the user. This is an important feature in reducing the cost of sale and improving customer satisfaction.

Supporting facilitated channels introduces the additional risk of internal fraud. To combat this threat, the security infrastructure must be capable of applying suitable controls on internal staff to restrict access and to monitor and report agent collusion.

The security costs associated with supporting a facilitated channel are therefore directly related to the complexity of services offered through each channel, coupled with the degree to which these security services are integrated with contact management applications and supporting infrastructures, such as Computer Telephony Integration (CTI).

1.3 Administration costs

In many organisations, users and customers must remember almost as many passwords as they have products; maybe more if they use multiple channels to contact the organisation. Where customers have more than one role, for example a retail account holder and business account holder, organisations tend to treat them as separate individuals. This means that the business often has to maintain multiple different identities and verifiers on different systems for the same user.

When customers forget a password, they are often forced use the telephone channel to perform a password reset, since facilities are not provided to reset their own passwords.

Due to the fragmentary nature of audit logs in a multi-channel, multi-role system, should there be a customer issue that requires an audit query, significant effort must be invested to piece together information from multiple records and systems.

The following are just some of the causes of costs that arise from having to maintain a user community served by the organisation:

- Resetting passwords;
- Re-issuing tokens or PINs;
- Enabling channels;
- Updating thresholds and access limits;
- Registering to access new services.

One way of arriving at a total cost of administration is to consider it in terms of the numbers of staff required.

For example: the cost of resetting passwords, which can account for up to 25% [Alle02] of all helpdesk calls, is significant. With speculative costs of £13 per call, a large financial services organisation serving 15 million customers has an average monthly call volume of around 4 million calls. This equates to a monthly bill in the region of £13million, just to reset users' passwords. Even considering the ambiguity of these estimates, the underlying message is that just servicing password resets is exceedingly costly and any actions that can be taken to reduce these figures will directly impact the organisation's bottom line. Statistics suggest that if a user has one password rather than five then the number of password reset calls is likely to fall by 80-85%

1.4 Operational costs

System costs associated with the deployment and maintenance of a single security solution can consider two main categories:

- Cost of implementation – these are the costs of delivering a security solution and include:
  - Physical hardware costs;
  - The cost of integrating with existing components;
  - The cost of changing internal processes and procedures often known as Business Process Re-engineering (BPR).
- Ongoing cost of system support – these are the costs of running and extending the solution once it has been delivered:
  - The cost of extending the solution – extending security services to support a new marketing initiative, an advancement in technology or a consolidation of services, sometimes means the costs of extending individual, point solutions becomes inhibitive;
  - Support and maintenance contracts – with multiple security services supporting the plethora of channels, products and services, the total ongoing support and maintenance costs are significant;

- Operational support – the staff costs associated with the daily maintenance of the system (the monitoring of logs, the maintenance of keys and daily housekeeping activities).

2 What is the ideal solution?

A Greenfield-site implementation has the benefit of no legacy system integration and the opportunity to deploy a security infrastructure capable of meeting the desired requirements. However, most real-world implementations are faced with a myriad of channels, services and, more pertinently, existing ID&V systems each supporting different parts of the business.

For example, a typical tier one retail financial services organisation is likely to be operating over 20 separate ID&V systems underpinning multiple products and services, which are used by in excess of 15 different, distinct customer communities. The underlying security infrastructure will comprise a complex mix of integrated, semi integrated and stand-alone systems, all playing their individual role in supporting discrete processes, service channels or user groups.

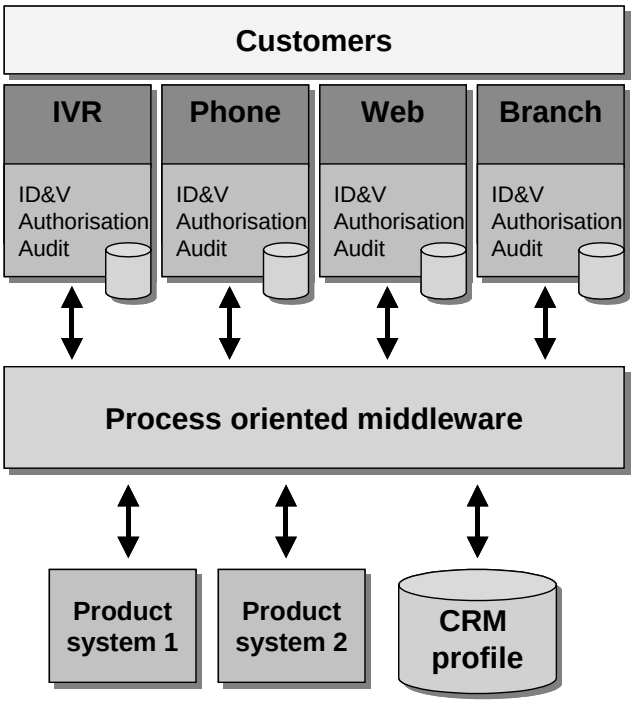

Figure 2: Silo approach to security services.

A much simpler and cost efficient solution is to implement a service orientated architecture (SOA) that adopts a single point of policy administration. This allows an enterprise-wide security policy to be deployed across an organisation administered from a single source.

Existing ID&V systems and services do not need to be replaced. The definition of user security profiles is consolidated into a central source, but the application of controls can continue to be enforced by existing services. A centralised security server provides the ability to deploy multiple security policies, concurrently from a single source. The solution provides extensible services to integrate to existing security solutions and data repositories.

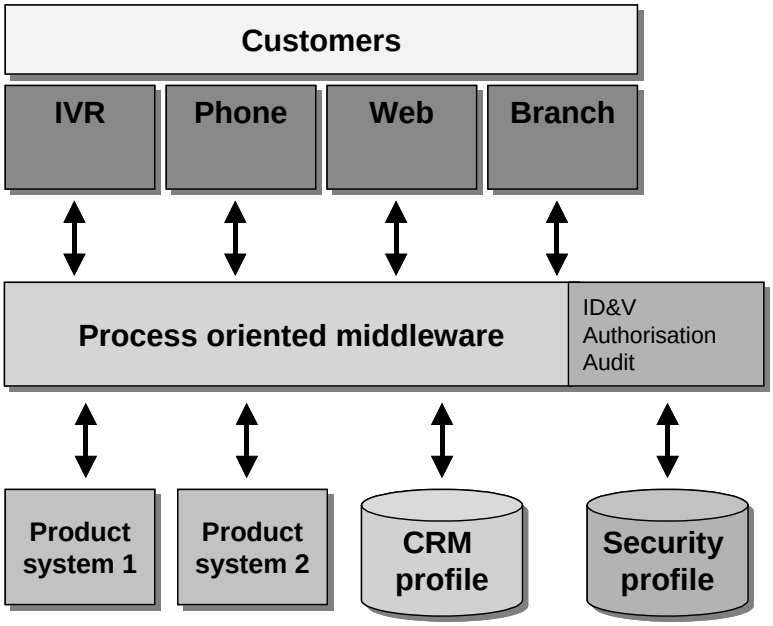

Figure 3: Multi-channel approach to security services.

This architecture has the following advantages:

- Maintainance of a single security service;
- A consistent application of security policies across all channels;
- Provision of a single source of audit data;
- Provides a framework for future expansion of security services;.
- Publishes a single set of security services that can be used by all registration systems, simplifying the provisioning process;
- Provides a a single security profile, with identifiers and verifiers that can be used across multiple channels improving customer experience.

3 How can cost savings be made?

The implementation of a solution that has a single point from which the enterprise security policy is defined produces significant cost reductions.

3.1 Registration

Reduction in the cost of registration – provisioning customers onto a security service using a single registration process and pre-registration for new-to-brand customers saves time and effort in channel-by-channel or service-by-service provision.

3.2 Servicing

Reduction in the cost of account servicing – facilitating the take up of lower cost channels and increasing call maturity – i.e. authenticating customers to a suitable level to enable agents to complete a customer request over the phone. With no process in place to allow customers to verify themselves to a level sufficient to perform an activity over low cost channels, customers are forced to complete the transaction either by post or face-to-face.

Reduction in the cost of sale – facilitating the hand-off between service agents and sales agents by pre-authenticating the customer and reducing the time taken by the agent in processing the sale.

3.3 Administration

Reduction in the cost of administration – Implementing a common ID&V solution across a large organisation, customers are less likely to forget passwords, lose tokens or mislay usernames. This has the direct impact of reducing the number of calls to support desks to reset or re-issue passwords immediately saving costs.

Simplified administration processes – by virtue of a single reset process administration processes are simpler and lower cost.

User self-maintenance – Adopting a security policy that provides users with back-up security mechanisms (such as memorable facts), empowers users to reset their own primary verifiers, reducing the number of administration calls and therefore operational costs.

Distributed administration – Having a security solution that can implement controls based upon user communities allows adminsitration of the user base to be delegated or outsourced.

3.4 Operation

Reduction in IT implementation and management costs – the costs associated with implementing and operating one, rather than many security systems (including annual maintenance, upgrade costs, systems operation, backup and recovery) is significantly lower.

4 Can security services increase revenue?

Although a security solution will not generate more income directly, enabling new processes and improving existing ones can have a significant impact on the bottom line.

Improved cross-selling – facilitating the hand-off of an authenticated customer between agents allows organisations to cross-sell through contact centres more efficiently.

Improves time to market – the ability to deliver new products and services to market, over multiple channels, quicker because of the underlying security framework.

Increased Customer retention – a single security process delivers improved customer experience and increased customer loyalty.

5 Intangible benefits?

The implementation of a centralised, common ID&V service that delivers an extendable framework for future verification mechanisms provides a number of intangible benefits such as:

Avoidance of further costs – Avoids the cost of implementing future verification mechanisms in multiple systems (e.g. two factor authentication using EMV smartcards). Avoid the cost of upgrades to existing security systems. Avoids the cost of implementing additional ID&V solutions for new products or services.

Technology

Identity Federation: Business Drivers, Use Cases, and Key Business Considerations

J. Matthew Gardiner

Netegrity, Inc.
201 Jones Road Waltham, MA 02451
Product Marketing Division
mgardiner@netegrity.com

Abstract

Finding ways to more efficiently and intelligently coordinate business and integrate business processes with trading partners to keep up with the ever-accelerating pace of business has long been a dilemma faced by many companies. Identity federation and the industry standards that comprise it were invented to address this cross domain, application interoperation challenge. This paper introduces and defines identity federation, the benefits that companies can reap by leveraging it, the typical use cases that can be enabled by it, the sometimes competing industry standards and specifications that underlie it, and finally the business issues that must be addressed for federated applications to be successfully delivered at scale.

1 Federation – Introduction & Business Value

Basic access to applications and data over the Internet has existed for years; however the ability for a user to easily and securely access services from multiple security domains within an enterprise or from multiple companies has remained a challenge. Finding ways to efficiently and more intelligently coordinate business with trading partners to keep up with the ever-accelerating pace of business has long been a dilemma faced by many companies. Twenty years ago many pinned their hopes on electronic data interchange (EDI), which has been used successfully in the automotive, retail, and manufacturing industries, but has generally failed to reach a broader corporate audience primarily because of its cost, inflexibility, and proprietary nature.

Today, the Internet, Internet-compliant technology, and standards have matured to the point that effective coordination and mass integration between trading partners is now achievable and affordable. Moreover, the advent of general purpose and industry specific standards are easing the extension of today's enterprises by lowering the barriers to connecting disparate business applications both within and across corporate boundaries. This enables businesses to substantially reduce costs, create new revenue opportunities, and provide greater convenience, choice, and control for its users.

By integrating applications and business processes across corporate boundaries, trading-partners, business customers, and outsourcers can automatically link processes and take part in transactions across multiple companies – eliminating the business interruption associated with traditional means of information exchange, such as phone, fax, and email. The ubiqui-

S. Paulus, N. Pohlmann, H. Reimer (Editors): Securing Electronic Business Processes, Vieweg (2004), 89-98

tous network (the Internet) and high-scale transactional applications already exist at most organizations. They can and should be further leveraged to drive cost and time out of doing business. Federation standards and the security systems that implement them were invented explicitly for this purpose.

2 Securing Federation

However, the aforementioned gains can fail to materialize if the information exchange is not conducted securely. For example, a government agency could risk damage through a leak of a citizen's private information. A financial institution might incur financial penalties and brand degradation due to an unauthorized trade or withdrawal. A health care firm might suffer damaging lawsuits with the release of personal health information to the wrong parties. With federation, as really with most IT efforts, organizations need to have security as a front-of-mind item. In the end though, a balance must be found between letting business in and keeping risk out.

In a federation scenario a key way to address these security challenges is to integrate partnering companies' security systems so that user, security, and entitlement information can be shared in a defined and controlled way between partners in a trusted business relationship. Integrating applications across independent security domains is defined broadly here as „federation". Furthermore, the sharing of digital identities to enable federation is defined as „identity federation". Federation enables users to work with autonomous internal business units, external business partners, and other third-parties seamlessly as if they were part of the same security domain, while in fact the domains remain largely independent.

Cleary, since cross-company federation is the ultimate goal, the only way to effectively accomplish this is through the development and use of open standards, since by definition multiple products will need to interoperate to deliver cross-company federations between given companies. Fortunately, many standards have and are being developed to address various aspects of identity federation (single sign-on (SSO), trust, attribute sharing, Web services security, privacy etc.). Some of these standards, when combined, provide the basis for an identity federation framework, but there are still overlaps and competition between emerging standards, making selection decisions challenging.

3 Federation Requirements

Given the intense focus on personal privacy and control of digital identities, the existing identity infrastructures that can be found in today's organizations, and the high-value of customer information that is often housed within them, it is virtually impossible to expect organizations to collaborate on creating and maintaining a universal, shared point of identity information. Requiring organizations to first merge their user's digital identities as a prerequisite to federating their applications for use by those users, is a non-starter. This is one of the basic requirements driving federation standards and why the space is termed „federation" (as in a „federal" government of individually sovereign states – as is the case in the USA) in the first place.

Companies involved in identity federations establish trusted relationships allowing their respective users to access resources operated by their business partners. To do this companies issue „security tickets" for their users that can be processed by relying business partners. Essentially, to over simplify, federation standards boil down to defining these security tickets;

what their structure is, what is in them, how they are passed, how they are administered, how they are validated, and what services they can and should enable.

4 Federation Use Cases

There are many potential federation use cases. The use cases presented in this paper are not intended to cover all the potential scenarios, but are intended to be generically illustrative of typical federation use cases to get the reader thinking about federation and how it may be leveraged by their organizations.

More specifically, identity federations can be conducted in two basic forms, browser-based or document-based. The browser-based mode of federation is focused on supporting live users that are using Web applications presented to them via standard Internet browsers. Federation in this case enables an authenticated user to move from one Web security domain to another without needing to provide credentials again. Browser-based federations essentially provide the user with SSO between two sets of applications or portals that live in two separate security domains, without requiring the synchronization of the user's digital identities in the two domains.

By contrast, document-based federations use XML documents transported between two security domains leveraging Web services. With document-based federations the activity is driven either by a live user sitting on some „client" application or by some client application in the absence of direct human involvement. Federations in document-based scenarios involve defining XML document structures, locations and definitions of credential information, and other factors.

Both modes of federation, browser-based or document-based, nonetheless hinge on the development and use of standards to simplify how two independent security domains can easily work together for the benefit of their common user.

4.1 Browser-Based Scenarios

The following use cases demonstrate different ways of using user identities to provide browser-based, end-users with SSO across multiple companies involved in a partnership.

4.1.1 Federation Based On Account Linking

In this use case, Workplace.com contracts the management of its employees' health benefits to a partner company called Health.com. To access her account, an employee of Workplace.com authenticates at the employee portal (www.workplace.com) and clicks on a link to view her health benefits at www.health.com. The employee is taken to Health.com's Web site and presented with all of her personal health benefit information without having to sign-on to Health.com's Web site.

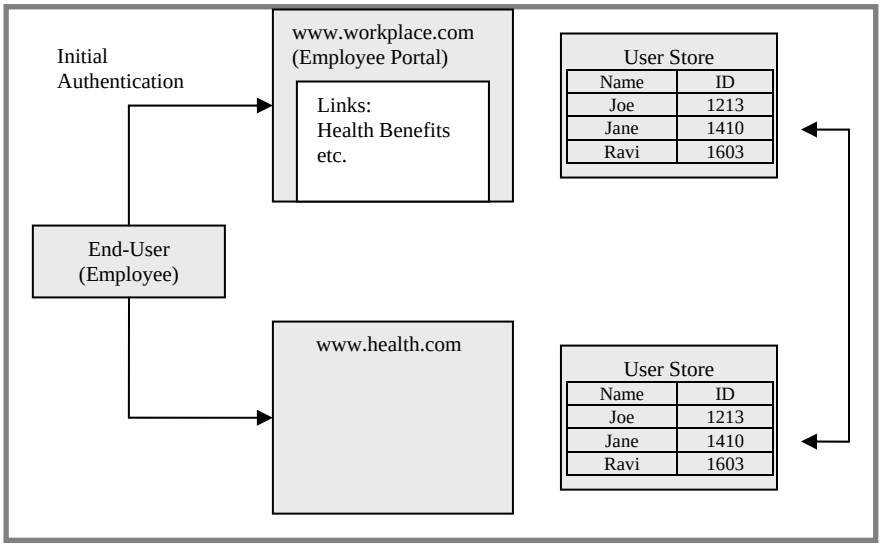

Figure 1: Federation Based On Account Linking

Health.com maintains all health-related information for the employees at Workplace.com. Health.com thus maintains user identities for every employee of Workplace.com a priori. When an employee of Workplace.com accesses Health.com as part of the federation an identifier for the employee is passed from Workplace.com to Health.com in a secure manner. This identifier allows Health.com to determine who the user is and thus what access to provide them. The security systems at Workplace.com and Health.com are linked (federated) to provide a SSO experience to their shared users.

Account-linking is the most typical browser-based use case being currently pursued by customers and prospects of Netegrity. However, the following additional use case is illustrative of another important browser-based federation scenario that is useful in some business situations.

4.1.2 Federation Based On Roles

In this use case Workplace.com buys parts from a partner company PartsSupplier.com. An engineer of Workplace.com authenticates at the employee portal (www.workplace.com) and clicks on a link to access information at PartsSupplier.com.

Because the user is an engineer (has the role of engineer) at Workplace.com, he's taken directly to the technical documentation and troubleshooting portion of PartsSupplier.com's Web site without having to sign-on.

In contrast when a purchaser for Workplace.com authenticates at Workplace.com and clicks on a link to access information at PartsSupplier.com they are taken directly to the order portion of PartsSupplier.com's Web site without having to sign-on.

In either case, PartSupplier.com's Web site can be personalized with information such as the user's name, leveraging whatever information is sent over from Workplace.com in the security token.

In this roles-based scenario PartsSupplier.com does not want to maintain user identities for all of Workplace.com's employees. However, PartsSupplier.com must control access to sensitive portions of their Web site. To do this, PartsSupplier.com maintains a limited number of profile identities (mapping to roles) for Workplace.com's users.

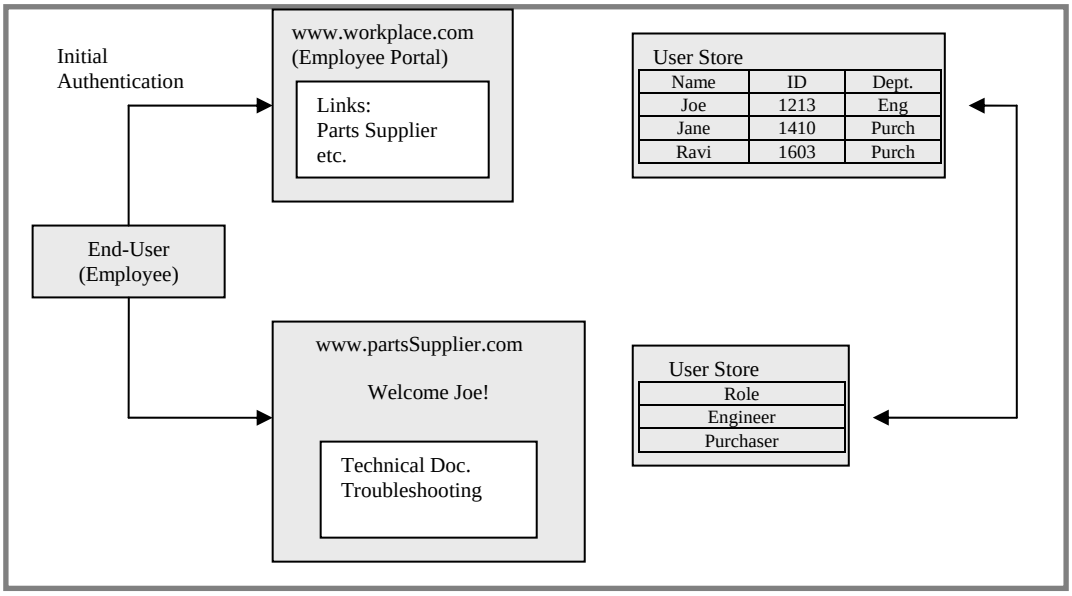

Figure 2: Federation Based On Roles

In this case, one profile identity is maintained for engineers and one profile identity is maintained for purchasers. When an employee of Workplace.com accesses PartsSupplier.com, user attributes are sent from Workplace.com to PartsSupplier.com in a secure manner, leveraging federation standards. These attributes define the role of the user and determine what profile identity is used to control access at PartsSupplier.com.

4.2 Document-Based Scenarios

Document-based federations are realized using Web services flows. As with browser-based federations there are many possible usage scenarios, I highlight one to convey the basic concepts that are involved.

4.2.1 Chained Web Services

In this use case, Workplace.com has a purchasing agreement with PinSupplies.com, and PinSupplies.com has a business relationship with E-Ship.com.

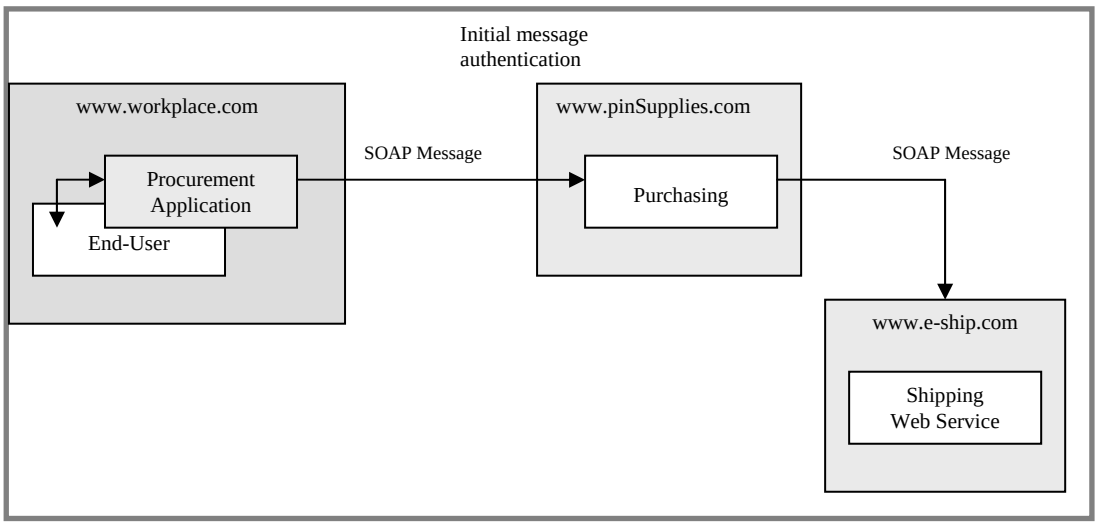

Figure 3: Chained Web Services

The end-user logs-on to her procurement application with her username and password. The procurement application provides a list of Workplace.com's various suppliers. The end-user clicks on the PinSupplies button and is presented with a purchase order in an HTML page. She fills out the purchase order and then clicks the submit button on the HTML form.

The procurement application turns the HTML form into an XML document that it inserts in the envelope body of a XML/SOAP message. The procurement application then inserts the end-user's credentials in the envelope header of the SOAP message, together with Workplace.com's organizational identity.

The procurement application posts the SOAP message to PinSupplies.com's purchasing Web service. The Purchasing Web service (or a security application on its behalf – the more scalable and manageable solution) authenticates the incoming SOAP message and processes the request. When the purchasing process is complete, the Purchasing Web service makes a request to E-Ship.com using a SOAP message. The SOAP message includes a PinSupply.com security token in the envelope header and the list of items to be shipped as well as the end-user's shipping information in the envelope body. The Shipping Web service (or a security application on its behalf) authenticates the request and processes the shipment order.

One of the keys to creating federated applications, as with any application really, is to think in terms of the users, what experience you are trying to provide them and how best to accomplish it, given your current infrastructure. When thinking about potential federated applications thinking in terms of browser-based versus document-based federations should help focus your thinking.

5 Key Federation Business Issues to Consider

While identity federation holds the promise of delivering significant benefits to users and organizations alike, the reality is that industry standards and specifications, such as SAML, Liberty Alliance, and others (discussed briefly below) can only go so far in resolving issues that are inherent when two or more organizations attempt to integrate their systems and business processes. The standards introduced below go a long way to make organizations' security infrastructures work together, but do not by themselves resolve the business issues inherent in federation. Early federation adopters will need to resolve the following issues, and probably others, in a form satisfactory to the federating partners, before they can launch their federation projects and scale them in any significant way.

- **Legal and contractual issues around trust** – Since federation implies that one-party depends on the security systems and practices of another party, any enabling contract needs to define what is required, what is expected, how liability is dealt with, what service levels are promised, what happens if and when there is a security breach, what controls does the partner have on providing user credentials, etc.
- **What happens when things go wrong, who does the user call?** – If a user can't get what they need for whatever reason, there needs to be a call-center or helpdesk that is equipped to help them and a process for managing customer issues that might originate with the federation partner.
- **What government regulations may apply? How can the partners ensure that they are complying?** – Depending on the industry, region of the world, and the personal data involved, different government regulations may apply. Which regulations apply and how to meet their requirements needs to be addressed as part of any identity federation.

- **Who pays for the federation?** – Given that by definition federated applications are shared and both sides often gain some benefit, it is not unreasonable to expect that both sides might need to pay for the federation to occur. How this gets sorted out depends highly on the existing economic relationship between the parties. It is certainly possible that one side or the other might handle all the federation costs, but this is clearly a non-technical issue that must be resolved before the specific federation can occur.
- **Privacy policy compliance.** – In most scenarios for federation to occur some amount of personal data about the user will need to be „shared" with the federation partner. Not only does this sharing need to be legal, but it also needs to comply with the privacy policies of both federating organizations.
- **Technical infrastructure/savvy of the federating parties.** – For two organizations to federate they need to integrate their security infrastructures using a standard of their mutual choosing. This assumes that both sides understand what that means and have the ability to acquire or build the required systems. Like any new technology, it is certainly recommended to start with the highest priority business partners that also have the highest level of IT and security expertise.
- **Scaling of the federation deployment** – While system scaling is certainly a technical issue, the engineers who are tasked with designing and deploying the federation infrastructure, on both sides, will need to be provided the business requirements regarding how many counter-parties will need to be supported, what the estimated transaction rate will be, and a number of other factors. The bottom line is this; the federation system that is built to support 1 federation counter-party might be dramatically different from that which would be required to simultaneously support 100 federation partners. The planned growth of the federated services will thus need to be addressed as part of the initial federation system design so that this system can scale to meet the organization's business needs.
- **Administration of the federated users** – Federation generally does not eliminate the need to administer the digital identities of the federated users on both sides of the federation. This administration requires more than a technical solution; it requires that organizations somehow create a cross-company process, perhaps enabled by identity management tools, that supports the digital identity data management. Said another way, organizations need to supply some process that supports the lifecycle of the user identity, from creation, modification, to ultimate deletion, for the federated applications of one or both parties.
- **Rights to audit federation partner** – Auditing and security systems naturally go hand-in-hand. Shouldn't one assume that this applies to federated security systems as well? However, given that one-half of the security system of the solution is housed at a business partner, getting access to their audit data (assuming they have it) is something that would have to be negotiated up-front.

The listing of the above business issues was not intended to scare the reader off from considering identity federation projects. It was provided to help set the right expectations for all participants. It is important to understand what business issues will have to be faced with identity federation in addition to the technical issues. Going into a federation project without addressing the business issues is a recipe for a disaster.

Like any new IT initiative in most organizations, effective execution of the first project is critical to making usage grow over time. Success breeds more demand, more funding, more attention, and hopefully growth of the initiative over time. The best advice I can give is to

pick your best, most motivated partner first. Get all aspects of your federation, both business and technical issues, right with them and then expand to more partners as time, demand, and resources allow.

6 Federation Standards

There is no single industry standard that meets all federation requirements, whether browser-based or document-based. As mentioned in this paper, federation involves description of identities (i.e., security tokens), protocols to exchange security tokens, preservation of privacy, and methods for the establishment of trust.

This section briefly describes four standards and industry initiatives that in the opinion of the author are most immediately important to identity federation and trust initiatives:

- SAML
- Liberty Alliance
- WS-Federation
- WS-Security

6.1 Security Assertion Markup Language (SAML)

SAML is an open, application-level, framework for sharing security information on the Internet through XML documents. In January 2001, Netegrity along with other companies, created the OASIS Security Services Technical Committee (SSTC) which culminated in the adoption of SAML as an industry standard in November 2002. SAML 1.1, the current version of SAML, was approved by the OASIS Board in September 2003. SAML is probably the single most important, supported, and implemented federation standard currently in existence.

6.2 Liberty Alliance

The Liberty Alliance Project (loosely referred to as Liberty Alliance or Liberty) is an industry organization started in September 2001 that currently includes over 150 member companies worldwide, including Netegrity. The purpose of the Liberty Alliance is to create a set of specifications for identity federation.

The ID-FF module is the foundation of the Liberty architecture and is the portion of Liberty most commonly in current use. I thus focus on it further.

6.2.1 ID-FF

A basic ID-FF environment minimally includes three parts: an identity provider (e.g., a telecommunication company), a service provider (e.g., an online retailer, a financial institution, a government agency), and a user agent. The user agent is a thin client (e.g., a standard browser) or a Liberty-enabled client or proxy (LECP), e.g., a wireless (cellular) telephone handset. Use cases under ID-FF fall into the Federation Based on Account Linking use case described in the Browser-Based Scenarios section above.

With ID-FF, upon successful authentication of the principal, the identity provider produces a SAML Assertion including an authentication statement describing the principal’s security context, together with a name identifier (or „handle”).

6.3 WS-Federation

Web Services Federation Language (WS-Federation) is a specification jointly developed by IBM, Microsoft, BEA, Verisign, and RSA. WS-Federation will no doubt be of interest to most readers since Microsoft has announced that a WS-Federation supporting product, formerly codenamed TrustBridge, will come to market sometime in 2005 and be called Active Directory Federation Service (ADFS). The plan as of this writing is for Microsoft to include ADFS as part of the Windows Server 2003 Update, codenamed R2.

WS-Federation provides support for secure propagation of identity, attribute, authentication, and authorization information. In many ways WS-Federation is quite similar to the SAML standard. WS-Federation enables brokering of trust and security token exchange, support for privacy by hiding identity and attribute information, and federated sign-out. The practical advantage of WS-Federation is with its future release in Windows, and the massive world-wide distribution that inevitably will follow, the ability to find technically enabled federation counter-parties will be dramatically improved.

6.4 WS-Security

The Web Services Security specification (WS-Security) was originally developed by IBM, Microsoft, and Verisign. It is now hosted by the OASIS Web Services Security Technical Committee (WSS TC). WS-Security specifies SOAP security extensions providing data integrity and confidentiality and is thus useful in the context of document-based federation scenarios. WS-Security defines how to attach signature and encryption headers to SOAP messages. It also provides profiles that specify how to insert different types of binary and XML security tokens in WS-Security headers.

7 Conclusion

Enterprises are faced with an increasingly complex set of challenges as they balance the need for security and the growing requirement for seamless access to information from a large and diverse set of users. Integrating partners and their heterogeneous security systems and infrastructures to securely share and administer user information, profiles, and entitlements requires a solution that supports scalable, inter-enterprise security that stretches across many partnerships. Federation standards and the security products that implement them are focused on providing exactly these services.

Today, the Internet, Internet compliant technology, and federation standards have matured to the point that effective coordination and mass integration between trading partners is now achievable and affordable. The immediate benefits of this are available to those organizations with the vision and the focus to take advantage of the building blocks and make it happen for their organizations. The question to the reader is how are you going to let business in while keeping risk out?

Application

Spam is Here to Stay

Andreas Mitrakas

Ubizen NV
andreas.mitrakas@ubizen.com

Abstract

Spam has emerged as a modern day threat to electronic communications networks. Spam affects governments, service providers, commercial and private users alike. Spamming constitutes a breach of privacy, consumer protection laws, cyber crime laws and can have severe consequences for the party apprehended. Law enforcement that currently remains a cross border issue has yet to be enhanced in order to allow for law enforcement. Cooperation among service providers and the implementation of technical methods is likely to also make an impact. Enhanced end-user awareness can alleviate the burden of managing the huge amounts of spam without, however, necessarily solving the problem. A significant break through can be sought in the direction of authentication mechanisms including electronic identities that protect privacy and allow for personalized services.

1 Introduction

Ever since it first emerged, spam has threatened the unfettered use and evolution of electronic services. The facility with which large volume of unsolicited commercial communications circulate on the Internet threatens the functionality of email that legitimate users seek. Spam threatens government, businesses and consumers alike in terms of wasted resources to manage spam and potential exposure to fraud that goes along with it. Riskier for all potential recipients of spam is the distribution of viruses. Recently, several legislative initiatives have attempted to check spam in a way that meets the expectations of the public and private users. Additionally, a number of self-regulatory initiatives and measures also aim at bringing spam under control. While the success of these initiatives has yet to be proven, spam has been on the rise with rates shunning the ones presented just a few years or even months ago. The remainder of this paper examines the background of spam, it presents legislative initiatives in the EU and US and it addresses future trends in an effort contain spam.

2 Background

On 12 April 1994, attorneys in Arizona launched a homemade marketing software program in the hope to attract extra business. A script that flooded online message boards with an advertisement pitching the legal services of a specific law firm has been singled out as the starting point of spam. Although less conspicuous spam attempts had already been recorded earlier intrusive online marketing has since then become almost an epidemic of massive proportions (See, www.templetons.com). While the recipients' response was immediate unsolicited mass email has persisted since then. According to a ZDnet report quoting a published estimation, almost 82% of all email traffic in the US and 50% worldwide is spam.

The definition of spam has sometimes relied on the term unsolicited commercial email. This definition poses some problems though due to the difficulty to define the meaning of the term commercial in this context. Since spam encompasses non-private communications of some-

S. Paulus, N. Pohlmann, H. Reimer (Editors**):** Securing Electronic Business Processes, Vieweg (2004), 179-185

times malicious intentions it can be argued that spam is not an exclusively business related phenomenon. The Data Protection Commission in France (Commission National Informatique et Libertés – CNIL) has defined Spam as: „The practice of sending unsolicited emails, most frequently of a commercial nature, in large numbers and repeatedly to individuals with whom the sender has no previous contact, and whose email address may be found in a public space on the Internet, such as newsgroups, mailing lists, directory or website". Spam is unwanted because it:

- Interferes with daily tasks and reduces the ability to work effectively.
- Clogs communications networks and uses up network bandwidth.
- Undermines consumer confidence.
- Poses risks for end users through the risky offerings that are associated with spam.
- Is equally threatening electronic as well as mobile communications.

The legal repercussions of spam are so severe that include breach of privacy, breach of confidentiality, computer crime, consumer law and personal data law violations etc. Taking action against spam has been considered a priority and several initiatives across both Europe and the US have attempted to bring spam under control. Spam for the infrastructure service providers, entails unauthorized user of capacity, increased costs for filtering, security costs and support for dismayed customers. Organizational users risk losing business, business opportunities, and risk productivity losses from within their own employees. Individuals lose their time, content and often fall prey to fraud instigated by unsolicited offers and identity fraud scams.

To their defense spammers claim that they influence the sales power of the end user away from big market players. Commercially speaking, spam's combination of anonymity, volume and low cost make it worthwhile for many to try reap the benefits by assuming the risk. The business of commercial spam is based on a customer base that seeks marketing its wares in an unsolicited manner. The list of recipents' addresses comes from agents that collect addresses from Web pages, newsgroups, chat rooms, and other online destinations. The spammer relies on Internet servers in places where there is weak or no legislation associated with spam and where they can relay their messages anonymously. Spammers' identity is typically covered behind a fake name. Dedicated mailing programs are also used to get spam messages out and are usually also equipped with stealth features that evade filtering and go unnoticed.

In an effort to detect and avert spam relayed through their infrastructure, internet service providers implement message filtering at a large scale. By using software that checks senders' Internet addresses against a database of known spammers and rejecting emails that contain predetermined keywords, ISPs strive to contain the amount of spam circulated. ISPs often prevent their services from being used as a spam springboard by limiting the number of recipients each message can be sent to. ISPs also set up reporting channels for their customers where they can forward spam emails for reporting and blacklisting.

Among the most widespread forms of spam the following top the ratings:

- Adult material sent out indiscriminately to adults and children alike has been singled out by the National Consumers League in the US as the most broadly used form of spam.
- An urgent and confidential letter claiming to originate from a former government official or a person in danger, typically from a troubled place in the world asks for the recipients banking details to transfer large amounts and to also benefit the recipient. Recipients who reply back are requested to send relatively small amounts of money for legal fees, etc., or their accounts are simply cleaned out.

- As online sales grow spammers propose items that might not exist, check from parties with dubious reputation. Paying by credit card could be a remedy against such scams.
- The practice of trying to lure Internet users into disclosing personal financial information such as credit card numbers through e-mail scams can cost financial institutions dearly. Identity theft or „phishing" involves sending bogus e-mails, set up to look like they are from online retailers or other businesses, asking consumers to send credit card numbers and other information [Mitrakas 2002]. Spam and phishing scams erode consumer confidence in electronic transactions.

In spite of the growing costs associated with spam and the increased suspiciousness of email users towards it the success of spam remains unfettered although:

- The interest in spam is next to zero.
- The content of spam does not appeal to end-users.
- Technological measures are implemented by ISPs.
- Legislation has been introduced in the EU, US and elsewhere.

3 Legislative initiatives

In 2002, to counterbalance the threats posed by spam the European Commission took action against it by adopting a Directive on Privacy and Electronic Communications. The Commission also works together with the data protection authorities from the Member States (Article 29 Working Party).

Directive 2002/58/EC of 12 July 2002 on Privacy and Electronic Communications aims at a pan-European „ban on spam" to individuals. With only a limited exception referring to existing customer relationships, e-mail marketing is permitted subject to prior consent of the end user (Article 13). Consent can be given by purchasing similar products in the past by the consumer. The definition of similar products and services as those originally bought by the customer is not addressed in the Directive [Reed 2000]. However, the same provision includes two supporting safeguards, namely that the data may only be used by the same company that has established the relationship with the customer in the first place and that each message must include an opt-out option. It is, therefore, expected that companies will have a strong interest not to abuse the notion of „similar products or services" and that in this case the customer is in a good position to stop marketing messages should such abuse occurs.

Interestingly and in stark contrast with other Directives that make a distinction between electronic and mobile communications, SMS messages and electronic messages received on any mobile or fixed terminal are equally sanctioned under 02/58/EC. However, fax is not included in this exception. This Directive sets an „opt-in" regime that end users can initiate. Member States can also ban unsolicited commercial e-mails to businesses, which do not fall within the initial objectives of the Directive.

The new rules introduced with Directive 02/58/EC, apply to the processing of personal data in relation with the provision of publicly available electronic communications services in public networks within the EU. An important distinction, therefore, is that article 13 that establishes the opt-in rule is applicable to all unsolicited commercial communications received on and sent from networks in the EU. Messages originating from third countries must also comply with the rules of the Directive. Obviously the same applies to any communications sent by an address within the EU to recipients elsewhere. As it can be expected, however the gravest difficulty is associated with the enforcement of the rule with regard to messages sent from ad-

dresses outside the EU. With most spam reaching EU based end users from addresses outside the EU, this is by far the most important matter for end users, which, however, the Directive does not necessarily address sufficiently.

Member States had until October 2003 to transpose a „ban on spam" into national legislation. Delays to meet this deadline have resulted in certain member states being brought by the European Commission before the European Court of Justice.

Directive 02/58/EC is not the first attempt of the EU Commission to check spamming. The data protection directive (1995/46/EC) grants protection to any personal identifiable information that might be abused. The 1995 Directive introduces an opt-out procedure to deal with spam. Certain types of personally identifiable information such as religion, ethnicity etc., are covered by more severe restrictions of processing. An opt-out register, however, could lead to abuse since it is a formidable source of email addresses.

The issue of „opt-in" or „opt-out" has been quite critical in the EU. Opt-in creates permission, which is not objectionable. The Data Protection Directive is relevant also because it establishes the right to claim damages as a result of spam. The Directive 95/46/EC sets out that penalties can be sanctioned for infringements of personal data. Beyond fines and possibly also criminal charges, other remedies for infringes of personal data currently include an injunction to cease unauthorised personal data processing. Additionally, spamming might result in breaching other obligations under the general data protection directive, such as the duty to notify for data processing etc.

The electronic commerce Directive (2000/31/EC) requires email to be clearly and unequivocally identifiable as such as soon as recipients receive it. Opt-out registers did not exist at the time of the Directive and were not forthcoming as a result of the legislation. Should, however, an end user contact a vendor to buy something online, that vendor can send additional information. With regard to business users the Directive stipulates that member states could require opt-out arrangements rather than opt-in. By contrast Directive 02/58/EC requires a soft opt-in with some exceptions. Finally consumer protection legislation in the EU also impacts spamming due to the requirements of transparency in communications and service offers emanating from Directive 97/7/EC on consumer protection in distance contracts [Hoernle et al. 2002].

Computer-related crimes are: „traditional crimes that can be, or have been, committed by using other means of perpetration which are now carried out through an Internet based computer-related venue (e.g. e-mail, newsgroups, other networks) or other technological computing advancement" [Trento 2002]. To investigate cyber-crime and crimes carried out with the help or by information technology, law enforcement agencies seek access to content of communications, data in transit, stored data and authentication data. The criminal law consequences of spamming might well qualify to be dealt with under the Cybercrime provisions. Article 15 of the Convention on Cybercrime of the Council of Europe stipulates that investigative powers and procedures are subject to conditions and safeguards provided for under its domestic law in a way that provides for adequate protection of human rights and liberties. The Convention on Cybercrime addresses computer-related offences that include computer-related fraud, which stands for „the causing of a loss of property to another by: any input, alteration, deletion or suppression of computer data, any interference with the functioning of a computer system".

In the US Federal Legislation entitled Controlling the Assault of Non-Solicited Pornography and Marketing Act (S.877) (CAN-SPAM) has been introduced to focus upon controlling unsolicited commercial electronic mail messages. CAN-SPAM has made illegal to send spam

that has false or misleading heading or origin information. Having a functioning return message capability and a physical postal address is essential because CAN-SPAM makes it illegal to send additional unsolicited messages to anyone who has indicated that they do not want to receive future messages from the sender. CAN-SPAM is an opt-out system but is also allows senders to provide „opt-in" to receiving certain kinds of email. ISPs who have posted notices stating that the web site or ISP does not store or transfer email addresses to any other party for unsolicited email purposes can benefit from CAN-SPAM.

Neither in the EU nor in the US seems to have been sufficient experience in enforcing the opt-in or opt-out rules for communications originating outside their respective territorial boundaries. It is a known fact that in cases of cyber-crime, international cooperation is critical in order to ensure the reconstruction of context and the collection of evidence. In the case of spamming international cooperation is needed in order to support the investigation on the identity of senders.

4 Self-Regulatory initiatives

User action has been a viable remedy against spam. In May 2003, the US based ISP, Earthlink, won a motion and a permanent injunction against a Buffalo, N.Y.-based sender of junk e-mail. Among other Internet providers, America Online has also sued spammers in a US federal court. AOL has won 25 spam-related lawsuits against more than 100 companies and individuals.

In *Compuserve v. Cyber Promotions*, 962 F. Supp. 1015 (S.D. Ohio 1997), the plaintiff, being Compuserve sued to enforce its contractual prohibition against mass electronic mailings. The defendant continued to spam even after being warned not to. Plaintiff successful sued under the theory of trespass to personal property.

In the early days of commercial Internet spamming had been largely considered unethical and dealt with in practice by trying to undermine the computers of the spamming senders. However, netiquette rules have currently a very limited influence on the day-to-day practice of commercial communications. Filtering software gave the next stage in ISPs fighting spamming however a common criticism is that often wanted email is filtered out together with unwanted email. Besides repeating offenders, one-time spammers pose an equally difficult problem much as resurfacing ones do.

To meet the goal of containing spam, building awareness could be considered as a step in the right direction. Creating user awareness on how to avoid or contain spam could have an impact to reducing the actual number of spam circulated in communications networks. Specialized end user software for the client or the server side that is anyway broadly available might also support awareness activities.

In general awareness of spam rights must stay in touch with the enforcement of data protection rights, an issue that still requires additional attention by the member states. The efforts of the French Data Protection Authority (CNIL) which is the national data protection authority have focused not just on the protection of personal data but they have made consistent efforts to ensure that spamming is somehow addressed and dealt with. The French Data Protection Authority has therefore, put up a web site that contains a significant amount of information package on spam such as basic guidance on how to prevent spam, information on how to report spam, users groups and associations active in this area, etc. Further action undertaken by public authorities, user and industry groups is likely to contribute to containing spam.

Practice

Managing Trust in Critical Infrastructure Protection Information Sharing Systems

John T. Sabo

2291 Wood Oak Drive
Herndon, Virginia 21401
USA
Computer Associates International
john.t.sabo@ca.com

Abstract

In North America and Asia Pacific countries, private sector companies, non-profit organizations and governments are developing partnerships to protect national critical infrastructures, such as electricity, energy, financial services, healthcare, information technology, telecommunications, transportation, and water systems. This paper discusses the operation in the United States of Information Sharing and Analysis Centers (ISACs), trusted information sharing systems which communicate alerts, vulnerabilities, and best practices and ensure coordinated incident response in critical infrastructure sectors. It describes operational and policy requirements and issues identified by the Council of Information Sharing and Analysis Centers (ISAC Council) for successful and trusted deployment of such information sharing systems, including the operational relationship of ISACs to U.S. government systems. It also discusses security and privacy issues which these systems must address to ensure widespread adoption and effectiveness.

1 Background

Globally, it has become increasingly evident that private sector companies, non-profit organizations and governments must develop partnerships to ensure national critical infrastructure protection (CIP) in such sectors as electricity, energy, financial services, healthcare, information technology, telecommunications, transportation, and water. Protection is needed from both cyber security and physical threats.

With upwards of 85% of such critical infrastructures owned an operated by private sector companies in the United States, Information Sharing and Analysis Centers (ISACs) have been established to provide 24 by 7 operational capabilities to communicate alerts, vulnerabilities, best practices, and threat information to members, to provide a coordinated incident response capability for their respective sectors, and to interface with government monitoring and analysis centers. ISACs were formally defined by then President William Clinton, in his 1998 Presidential Decision Directive 63 (20 May 1998) following recommendations of a Presidential commission studying critical infrastructure protection issues. In the current administration, President Bush's Homeland Security Presidential Directive-7 (HSPD-7), the emphasis on public-private sector information sharing continues:

S. Paulus, N. Pohlmann, H. Reimer (Editors): Securing Electronic Business Processes, Vieweg (2004), 271-280

> *„The Department and the Sector-Specific Agencies will collaborate with appropriate private sector entities and continue to encourage the development of information sharing and analysis mechanisms. Additionally, the Department and Sector-Specific Agencies shall ... identify, prioritize, and coordinate the protection of critical infrastructure and key resources; and ... facilitate sharing of information about physical and cyber threats, vulnerabilities, incidents, potential protective measures, and best practices."* [HSPD03]

With a number of ISACs now operational in the United States, the security, privacy, and trust issues they have begun to identify can provide valuable lessons as the ISAC model is explored internationally.

Because they are private-sector based, ISACs have very different organizational, funding and trust models, reflecting differences in their sectors. For example, certain ISACs are operated and managed by existing industry organizations (such as the Electricity ISAC), some are independent non-profit corporations (such as the Information Technology ISAC), and some are organized in partnership with government (Telecommunications ISAC). This diversity has prevented the development of a consistent ISAC operational model. Nevertheless, there are common issues affecting ISAC operations and their ability to interoperate effectively with one another and with government, particularly the Department of Homeland Security, which holds primary responsibility for critical infrastructure protection for the United States government.

Representative ISACs and their primary sponsoring organizations are shown in the following table:

Sector	**Principal Organizers**
Chemical	American Chemistry Council and other industry associations
Electricity	North American Electric Reliability Council (NERC)
Energy	American Gas Association and American Petroleum Institute
Emergency Management and Response	U.S. Federal Emergency Management Agency (FEMA)
Financial Services	The banking, securities and insurance industries
Highway	American Trucking Associations
Information Technology	Leading information technology companies, including Computer Associates, CSC, General Dynamics, Microsoft
Public Transit	American Public Transportation Association
State Government	Multi-State ISAC, New York State
Surface Transportation	Association of American Railroads
Telecommunications	National Coordinating Center for Telecommunications (NCC) with industry participation
Water	Association of Metropolitan Water Agencies

2 ISAC Council

To provide a forum for cooperation, 14 ISACs have come together as an ISAC Council. Members are Chemical, Electricity, Emergency Management and Response, Energy, Financial Services, Healthcare, Highway, Information Technology, Multi-State, Public Transit, Research and Educational Network, Surface Transportation, Telecommunications, and Water. More detailed information is available at www.isaccouncil.org. The mission of the ISAC Council is to „advance the physical and cyber security of the critical infrastructures of North America by establishing and maintaining a framework for valuable interaction between and among the ISACs and with governments."

In addressing this broad mission, the Council has undertaken a number of efforts: to identify and resolve ISAC community issues, especially ISAC operations and operational policy; maintain and enhance inter-ISAC coordination; establish and maintain a dialogue with the governmental agencies that deal with ISACs; develop a practical data and information sharing protocol; develop analytical methods to assist the ISACs to support their own sectors and the other sectors with which there are interdependencies; and identify and disseminate knowledge and best practices.

The ISAC Council has had significant success in working across sector lines and with the department of Homeland Security. One of its key tasks has been to formulate a working definition of an ISAC as a starting point for understanding the private sector's responsibilities for CIP. Key components of that definition establish an ISAC as a trusted, sector specific, entity which:

- provides a 24-hour/7-day secure operating capability that establishes the sector's specific information and intelligence requirements for incidents, threats and vulnerabilities
- collects, analyzes, and disseminates alerts and incident reports to its membership based on its sector focused subject matter analytical expertise
- helps the government understand impacts for its sector;
- provides an electronic, trusted capability for the membership to exchange and share information on cyber, physical, and all threats in order to defend the critical infrastructure, and
- provides analytical support to government and other ISACs regarding technical sector details and in mutual information sharing and assistance during actual or potential sector disruptions whether caused by intentional, accidental or natural events.

Sector focus, analytical capability, secure, trusted 24x7 operations, and collection and dissemination capabilities are the key components of this definition, and help distinguish ISACs from other organizations having a different role to play in critical infrastructure protection. For example, some organizations do not have staff capable of analyzing vulnerability and threat information against a specific sector's operational environment, or do not have the capability of generating new, sector focused information for distribution to their members, other ISACs and government. Such organizations, however valuable, would not meet the ISAC Council definition.

Given these characteristics, the importance of ISACs as a trust community cannot be underestimated. Their success, both in private sector terms and from the government perspective, will be based on their capability of ensuring adherence to information sharing policies, identifying and authenticating participants in their networks, reaching broadly into their sectors, and providing value to members. However, such a public-private trust community with such a broad

national security mission has not existed before, and a number of issues need to be understood and addressed if it is to be successful. The ISAC Council has begun to undertake this effort.

3 Trusted Information Sharing: White Papers

The ISAC Council has established regular meetings for issue resolution, provided a central contact point and mechanism for interaction with the Department of Homeland Security, worked with DHS to establish an Emergency Notification System for crisis response, and identified trusted information sharing mechanisms and networks that will work in private sector environments. With respect to this last area of focus, a key initiative has been the identification of barriers to trusted information sharing among ISACs and government and the preparation of eight issue papers (white papers) to identify barriers and where possible propose solutions.

As a principal co-author of one white paper, and as contributor and reviewer for the others, I believe it is important to understand the policy and operational trust issues raised in the papers. I recommend reading the papers directly (available at www.isaccouncil.org. It is important to note that the papers reflect the collective analysis of members of the ISAC Council in addressing issues of concern to ISAC operations and do not necessarily reflect all the operational structures used for CIP by the sectors (in some instances sectors have other protection mechanisms in addition to ISACs).

The private sector emphasis is important in the U.S. environment. However, many of the white papers identify issue and suggest approaches to problems that would be relevant in many countries which have de-regulated critical infrastructure industries and where government cannot implement solutions without private sector cooperation.

Taken together, the papers are beginning steps in tackling serious policy and process issues challenging the implementation of an effective private sector and government information sharing and analysis partnership and in fact are a catalyst for additional work to resolve the critical issues they identify.

4 The ISAC Council White Papers

The white papers are listed below, along with a short abstract describing the key issues which they address [ISAC04].

4.1 Government-Private Sector Relations

This paper addresses coordination and communication between the government and sectors, coordination and communication among the ISACs, incident data sharing, analytical information sharing, communications including mechanics and protocols, physical and cyber interdependencies between sectors, and research and development requirements.

4.2 Homeland Security Presidential Directive 7 (HSPD-7) Issues and Metrics

Homeland Security Presidential Directive-7 (HSPD-7) establishes a national policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks. Although primarily focused on Federal agency responsibilities for critical infrastructure protection, it also establishes expec-

tations related to government interaction with the private sector. The ISAC Council has examined the current status of privately owned and managed critical infrastructure protection in the United States and identified a number of areas in which collaborative work with the private sector is necessary if the broad expectations raised by HSPD-7 are to be realized.

4.3 Reach of the Major ISACs

This paper describes the degree of penetration or reach into the United States economy and infrastructure for each ISAC. It is designed to assist provide an understanding of the value of the ISACs in currently reaching into approximately 65% of the infrastructures of the United States economy held in private hands. The potential goal for the ISAC communities, as they mature, is to reach nearly 95% of those U.S. private infrastructures.

4.4 Information Sharing and Analysis

This paper is an effort to establish a path forward and future vision for information sharing and analysis and to provide a functional model for Critical Infrastructure Information Sharing and Analysis. Based on various government and critical infrastructure meetings during the fall of 2003, it addresses a number of objectives, including increased information sharing and analysis, security efforts to support the broadest possible reach both within and outside critical infrastructures so that no entity is excluded and to ensure long-term viability, realize cost efficiencies, and reduce redundancy, where possible.

4.5 Integration of ISACs into Exercises

The United States government has been planning and conducting exercises to test the readiness of CIP and Homeland Security systems and stakeholders. However, there has been little to no integration of active private industry infrastructure into these exercises. In certain instances, private industry participation in the scenario was simulated. There has been no ISAC involvement in these national level exercises. The ISACs and private infrastructure must become fully integrated into these exercises. Private industry must become a critical element of these training exercises, which are a key element of both homeland security and homeland defense training.

4.6 ISAC Analytical Efforts

ISAC analysis should consider both physical and cyber security, and should address immediate, mid, and long-term information and intelligence requirements. The current and planned analytical capabilities of the various ISACs must be understood as a baseline for further inter-ISAC coordination and interaction, with the analytical strengths of the ISACs providing the basis for further inter-ISAC cooperation. Government sponsorship and support of these analysis efforts must be considered and encouraged. A model that integrates private industry into the government intelligence cycle should be adopted.

4.7 Vetting and Trust

Efficient and effective processes for sharing critical infrastructure and security information on a timely basis must be developed. These processes must address the flow of information within an ISAC, among individual ISACs and between ISACs and government agencies. The processes must ensure that the information is available to the appropriate people, while providing reasonable assurance that the information cannot be used for malicious purposes and is

not indiscriminately re-distributed so as to become essentially public information. The ultimate effectiveness of these processes will be determined by the trust relationships that are established among the organizations participating in the information sharing.

4.8 Policy Framework for the ISAC Community

The policy areas discussed in this paper are those that directly relate to fundamental ISAC functions and that cross ISAC and government boundaries: to report and exchange information concerning incidents, threats, vulnerabilities, solutions and countermeasures, best security practices and other protective measures, in accordance with national critical infrastructure protection policy, and to establish a mechanism for systematic and protected exchange and coordination of such information. To make information sharing real, it is essential to lower the practical risks of sharing information through both technical means and policies and to develop internal systems capable of supporting operational requirements without interfering with core business. Consequently, the technical means used must be simple, inexpensive, secure, and easily built into business processes. The policy framework must reduce perceived risks and build trust among participants

5 A Common Theme: Trust

Despite their focus on different issues, a common theme addressed in the papers is how to establish – from the private sector perspective – a trusted, information sharing network among private sector companies and government to manage and coordinate vulnerability, threat, alerts, response, remediation and risk mitigation and analytical information affecting the common national good and do so in a way that actually provides a measurable level of protection.

A fundamental issue running through many of the papers is that of trust – what is needed to build trusted, secure information sharing systems among ISACs and with government. This is not an in considerable issue, since the effectiveness of information sharing for CIP purposes must depend on the timelines and accuracy of sensitive vulnerability, remediation and threat information *and* the ability to provide that information to the right organizations for appropriate action. In effect this requires establishing strong operational security and privacy policies and auditable controls.

5.1 Three ISAC Information Sharing Issues

Three fundamental issues are now emerging and being examined by ISACs with respect to information sharing within sectors, across sectors and with the government:

- **What information is needed** for sharing within ISACs, across ISACs and with the government, and how should this information be collected, stored, processed and communicated? -- *For example, when is it appropriate to share „raw" data and to whom, versus sharing aggregated data or analysis? Is classified information needed by ISAC operations centers?*
- **What kind of analysis and reporting** is needed and how is this shared with participating organizations (ISACs, U.S. governments, member companies, international governments) and with their members and employees? -- *For example, who should have access to the most sensitive analysis? Should there be „executive" and other role-based views of information, in addition to the network/security operations center view?*

- **What controls** must be put into place to protect the shared information – both in terms of personal and business privacy as well as information security? -- *For example, how are cross-jurisdictional authentication policies, data classification rules, privacy management and technical security and audit controls to be systematically addressed?*

All three issues are critical for building trusted CIP systems and are being addressed by ISACs and government. However, even as work is underway to answer the first two sets of questions, we must begin understanding the personal and business information security and privacy risks inherent in building CIP information sharing and analysis systems, develop appropriate policies to mitigate those risks, and identify appropriate procedural and technical controls to implement those policies.

5.2 Security and Privacy Trust Components

The following discussion of security and privacy risk management in information sharing systems is adapted from [Sabo04], p. 4-8.

5.2.1 Managing Security Risk

In the information security field, there exists a generally accepted body of knowledge available to practitioners to address most security requirements, including general policies; codes of security practices and lifecycle security models; security technologies, tools, products, and services; and audit instruments and technologies. While all of this capability will be critical to effective implementations, it is useful to examine four specific areas of security to guide initial thinking about how to build a trusted information sharing infrastructure.

Generally, information security controls in the ISAC context must include threat management, identity management, access management, and a security management capability (the latter to provide a comprehensive view of the network, systems and applications from a security perspective and enable effective security management). Given the distributed nature of the systems interacting in a national CIP system (companies, intra-ISAC, inter-ISAC systems, ISAC-government systems, and government-government systems), all of the following components must be used to build a trusted foundation for information sharing.

Threat Management controls protect networks and systems against external and internal threats, assess vulnerabilities, and they identify and mitigate physical- and systems-based risks and attacks – in effect, protecting the CIP infrastructure itself.

Identity Management controls provide a foundation for provisioning users and for role-based access, enabling role-based and portal views of information and applications. Uniform policy development will be necessary given the number of different organizations involved in the various ISAC and government organizations.

Access Management protects classified, regulated and business-sensitive resources; controls how resources are accessed and used; and ensures authorized availability across networks, systems and platforms. For ISAC purposes, „tiered" controls will be needed to reflect roles, information classification requirements, and particular organizational rules for information and for participants throughout the web of participating organizations and users. This is an important consideration, given the move toward defining one or more new classification categories for sensitive, „critical infrastructure information" falling outside the scope of Secret, Top Secret and other established national security classification levels.

Security Management capability is needed to effectively manage the security of the networked infrastructures. Included in this capability are resource management, impact correlation, secure collaboration, intelligent visualization, and predictive analysis tools.

Although further work is clearly necessary to improve our understanding of security risks and controls in the ISAC- government information sharing environment, the technologies, tools, practices and other components for addressing information security requirements are understood and available in the marketplace. However, to date, very little cross-sector and government-private sector work has been done to develop necessary policies.

5.2.2 Managing Privacy Risk

Understanding business and personal privacy risks, and then using appropriate and available policies and technical controls to mitigate them, are another important issue. For purposes of this paper, privacy is used as a broad technical term to include essential privacy principles such as those required under the U.S. Privacy Act of 1974:

- Identify and publish systems of records
- Inform individuals about the purpose the data was collected, their rights, the benefits of having the data, the obligations of the agency to protect the information
- Provide reasonable safeguards regarding disclosures and protections against security and integrity threats
- Maintain accounting of all disclosures of information except Freedom of Information Act and agency personnel who have need to know
- Assure records are accurate, relevant, timely, complete
- Permit individuals to access and amend their records

Information privacy management, as a technical discipline has, to date, achieved very little formal structure. In addition, aside from attempts to develop narrow technologies to address very specific privacy requirements (such as W3C's P3P standard [P3P] for expressing „notice" requirements), there are, as yet, no generally accepted and open standards-based architectures, protocols, languages, or schemas to ensure that privacy rules and policies can be embodied in IT systems or interoperate across networks that manage the lifecycle collection and processing of information. And yet both personal privacy as well as business privacy requirements must be engineered into the new cyber security architecture in order to enable the deployment of trusted systems.

An example of business privacy requirements in the ISAC environment is the formal IT-ISAC membership agreement (see www.it-isac.org). This agreement, signed by all members of the IT-ISAC, includes a number of rules for processing information, defined in a set of categories that the ISAC members must honor. Instantiating such business privacy requirements in networked information sharing systems will require an infrastructure capable of ensuring that data and information moving within and across ISACs and government systems are collected, processed, stored and communicated in accordance with defined business privacy processing rules. Additionally, it is important to note that the security controls noted in the prior section are necessary to support the security requirements of privacy policies. However, many privacy requirements exist outside the realm of information security, and include such things as „notice," „policy enforcement," „collection limitations," „re-disclosure constraints," and „individual access."

Considering the additional complexity of business privacy rules established by individual ISACs, their member companies, and governmental agencies (including State and local governments), it becomes obvious that building a scalable information-sharing infrastructure must address the automated management of differing (and perhaps at times conflicting) privacy rules and agreements.

Because currently available technologies can support it, an effective starting point may be the application of a broad privacy management framework, such as the Privacy Services Framework (v.1.1) developed by the International Security Trust and Privacy Alliance [ISTPA], a non-profit business alliance addressing privacy from a technology perspective.

Using the ISTPA Framework, cross boundary policies and operational requirements can be addressed by policymakers and system architects through a number of defined services and capabilities:

- ***control and data usage*** functionality, to ensure that policies drive business rules processing
- ***certification*** of system credentials
- ***validation*** of data
- ***interaction*** of data subjects, systems and processes
- individual and business ***access*** to data as well as ***audit*** capability
- use of ***agents***
- ***negotiation*** where appropriate.
- ***enforcement*** of policy violations

Many of these Framework services can be supported by currently available technologies in business intelligence, data management, enterprise management, and storage management, particularly when applied to enterprise implementations of data sharing systems.

However, in cross-sector and government-ISAC networked systems**,** these technologies should be utilized within an interoperable privacy architecture. In this context, the ISTPA Privacy Framework can serve as a tool for developing a model for the IT-based automation of privacy rules across the full lifecycle of information and across multiple jurisdictional (government, ISAC, corporate) boundaries. It can be used as a foundation for the collaborative development of architecture of privacy management.

6 Conclusion

If we accept the importance of critical infrastructure protection as a national security priority, and also accept that both private sector companies and governments have mutually dependent roles in building such protection systems, then the work of the ISAC Council in the United States can be seen, however incomplete, as a valuable beginning. The ISAC Council white papers provide an understanding of key information sharing issues and address the mutual roles and responsibilities of government and the private sector in establishing CIP systems.

Central to those systems is trust. Without trust among all participants, CIP systems will not be able to achieve their potential and will not effectively support national security and private sector goals. And without careful attention to security and privacy risk issues, including development of appropriate policies and implementation of adequate operational controls, trusted public-private sector information sharing systems will not be possible on a national scale.