facis

Zero Trust in Federated Cloud-Edge Ecosystems

eco

Funded by
the European Union
NextGenerationEU

Supported by:

Federal Ministry
for Economic Affairs
and Energy

on the basis of a decision
by the German Bundestag

8ra CLOUD·EDGE CONTINUUM

Version 1.0 (February, 25 2026)

ISBN: 978-3-9828074-2-3

Published by

eco – Association of the Internet Industry (eco – Verband der Internetwirtschaft e.V.) Lichtstrasse 43h, 50825 Cologne, Germany

Comissioned author:
Institut für Internet-Sicherheit – if(is)
Westfälische Hochschule
Neidenburger Straße 43
D-45897 Gelsenkirchen

Telefon: +49 (0) 209 95 96–515
Point of contact: Dr. Norbert Pohlmann & Daniel Theis
E-mail: pohlmann@internet-sicherheit.de
Website: https://internet-sicherheit.de/

Peer reviewed by the following persons in February 2026:

Andreas Weiss, eco – Association of the Internet Industry

Executive Summary

Today, digital collaboration is highly relevant to Europe's economic success. Organizations no longer work alone; they build value in dynamic networks across borders and industries. Data moves constantly between cloud platforms, factory floors, and mobile devices. This **new reality demands a new approach** to how we handle **security and trust** in fragmented, self-determined ecosystems.

Traditional security models rely on fixed boundaries and assume that trust begins once access is granted. It assumes everything inside is secure and everything outside is a threat. When you rely on trust within a boundary, you might lose control over systems, applications, and data.

To overcome such silos and build collaborative ecosystems, **two new concepts** are emerging: **Federation**, as a framework for a partner system with joined objectives and rules, and **Zero Trust**, which means no trust by default or within a certain perimeter. This paper introduces two core pillars:

1. **Federation** connects you without taking control. Think of it as a set of shared rules that allows different systems to talk to each other. You keep your data and your autonomy. You share access, not ownership.
2. **Zero Trust** protects every single move. It follows one simple rule: **"Never trust, always verify."** Every request to access data is checked in real-time. It doesn't matter who asks or where they are – the IT system validates the identity and the need every time.

The Business Impact: Why this matters for you

- **Move Faster:** Onboard new partners in days, not months.
- **Stay Independent:** Collaborate globally without being locked into a single provider.
- **Own Your Data:** Keep sensitive information at its source while still putting it to work.

- **Master the Edge:** Secure your operations where they happen – on the machine, in the vehicle, or at the hospital.

The Future: Europe thrives on specialized, distributed industries. Our economy needs a model that respects independence while enabling massive scale. Initiatives like **8ra** and **FACIS** prove that this works. They provide the blueprint for a digital landscape that is open, sovereign, and secure by design.

Zero trust and federation are leadership choices, not just IT projects. They determine how you compete, protect your IP, and scale your business. Do not leave trust to chance. Design it into your strategy to build a **resilient, fast, and truly sovereign future**.

Table of Contents

Table of Figures

Table of Tables

1. Why Digital Collaboration Must Change

Europe's economy requires transitioning from isolated operations to dynamic, distributed digital ecosystems. While value creation now occurs across organizational and national boundaries, many legacy IT systems still rely on outdated assumptions of stable environments and clear perimeters. To maintain competitiveness and security in this new reality, organizations require a new foundation for cooperation.

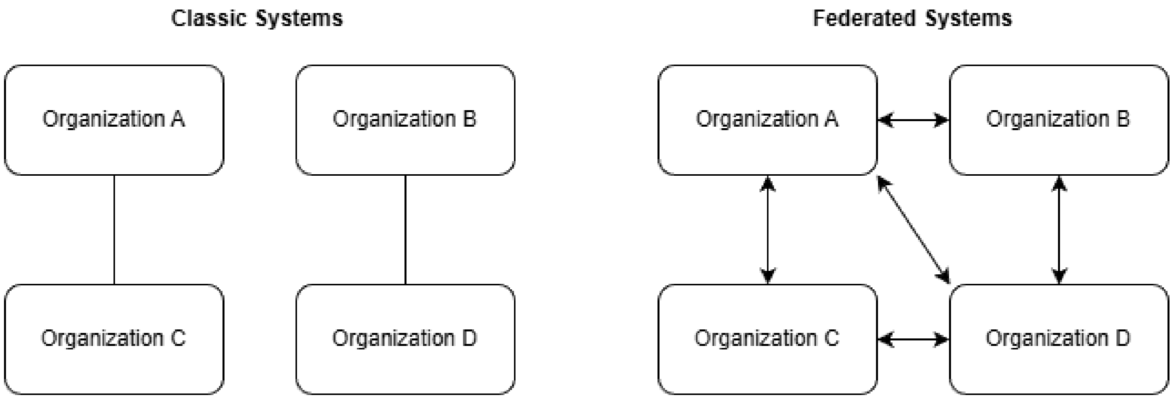

Figure 1 Classic vs. Federated Systems.

1.1 The Shift to Distributed Ecosystems

Digital work and data generation are increasingly decentralized, spanning cloud platforms, local IT, and edge environments.[1] Real-time requirements in sectors like manufacturing, mobility, and healthcare demand immediate, local processing.[2] In this connected landscape, digital infrastructure evolves from a mere application host into the active backbone of modern cooperation.[3]

[1] https://prace-ri.eu/wp-content/uploads/Edge-Computing-An-Overview-of-Framework-and-Applications.pdf

[2] https://elijah.cs.cmu.edu/DOCS/satya-edge2016.pdf

[3] https://www.globallogic.com/wp-content/uploads/2024/04/edge-computing.pdf

1.2 The Scalability Gap of Isolated Systems

Current isolated IT approaches fail to scale because each new partnership requires costly, manual integration and a manual rebuild of trust. These models often rely on static agreements rather than verifiable conditions, making them fragile as ecosystems expand. A sustainable model must enable reliable interaction between independent actors without sacrificing their autonomy.[4]

1.3 The European Perspective: Sovereignty and Openness

For Europe, digital collaboration must reflect a diverse industrial landscape without forcing centralization or dependence on a single platform. The goal is individual digital sovereignty: organizations must retain control over their data and identities while ensuring interoperability through shared standards. This sets the stage for federation as the primary model for cross-border cooperation.

1.4 Trust as the Central Challenge

In distributed ecosystems, trust is the decisive factor. Traditional security models with fixed boundaries are insufficient for dynamic environments. Establishing trust across borders and infrastructures without central control requires two components:

1. Federation as the structural model for cooperation.[5]
2. Zero Trust as the operating principle to ensure reliability.[6]

[4] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeLeitlinien/Zero-Trust/Zero-Trust_04072023.pdf

[5] https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf

[6] https://norbert-pohlmann.com/wp-content/uploads/2022/11/eco-studie_security-und-digitale-identitaeten-in-einer-digitalisierten-welt-prof-norbert-pohlmann.pdf

2. Federation: Connecting Without Centralizing

Federation is not a technology, but a conceptual model for cooperation. It allows independent actors to work together without being forced into a single system or under one central authority. Each participant retains control over its own IT environment, data, and rules, but can act jointly with other partners, based on agreed governance and interoperable IT and Identity systems.

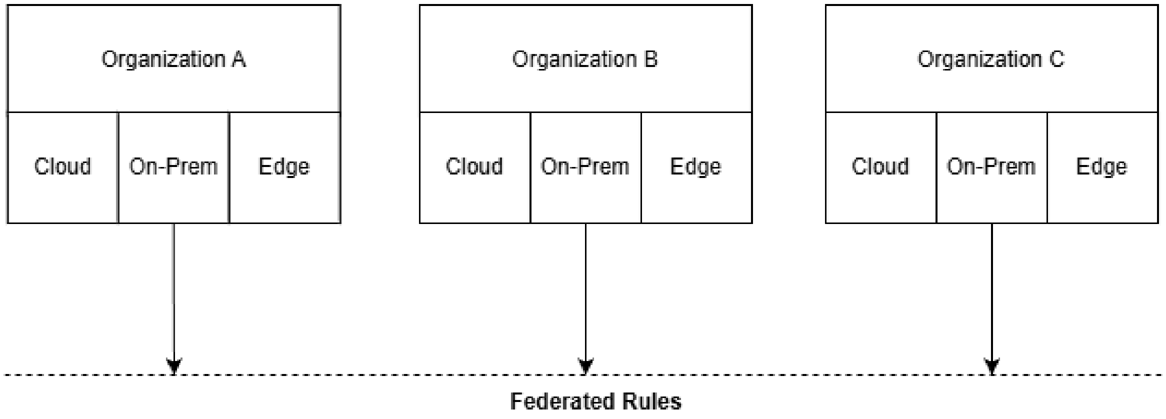

Figure 2 Connection Based on Federated Rules.

2.1 Principles of Federated Cooperation

In a federated setup, access replaces transfer. Cooperation is based on shared principles and standards, not on uniform technology. This ensures that organizations can collaborate while maintaining their autonomy and fulfilling regulatory requirements.[7]

In practice, participants agree on common ways of working together. These agreements define how interactions happen, what information can be used, and under which conditions access is allowed. Cooperation works because everyone follows the same principles – not

[7] https://gaia-x.eu/wp-content/uploads/2024/05/An-Introduction-to-the-Gaia-X-Trust-Framework_2024-V4.pdf

because everyone uses the same systems. This makes federation especially valuable where data is sensitive, regulated, or critical to the business.[8]

2.2 Federation as a "System of Systems"

Federation creates what can best be described as a "system of systems." Each organization operates a complete IT environment of its own. These environments differ in technology, structure, and maturity. Federation connects diverse IT environments through well-defined points rather than standardizing them. This approach respects the technological diversity of participants and allows ecosystems to grow: new partners can join without a complete redesign, and existing ones can evolve at their own pace.

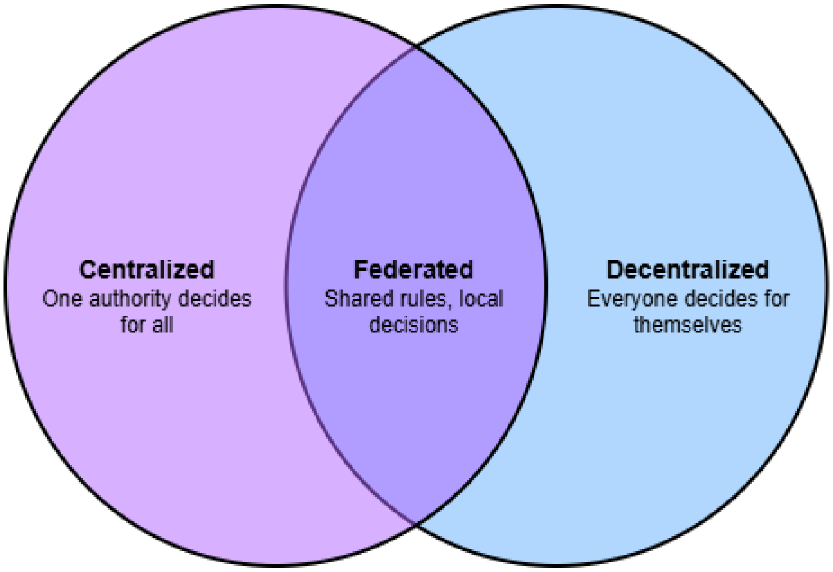
Centralized
One authority decides for all
Federated
Shared rules, local decisions
Decentralized
Everyone decides for themselves

Figure 3 Data Governance Model.

2.3 Federation vs. Central Platforms

While central platforms offer convenience, they often lead to dependency and strategic risk. Federation avoids "lock-in" effects. Decisions remain distributed, and no single actor controls

[8] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207A.pdf

the ecosystem. This makes federation the ideal model for complex, cross-sector, and international collaboration where digital sovereignty is a priority.[9]

2.4 Resilience and Participation

Federation lowers the barriers to entry for organizations of all sizes. By avoiding single points of failure and dominance, it increases the resilience of the entire ecosystem. However, a federated model without a central authority raises a vital question: How can trust be established across boundaries? This leads directly to Zero Trust as the necessary operating principle.

3. Zero Trust: Concept to Operating Principle

Federated digital ecosystems require appropriate trust mechanisms. Organizations depend on systems and partners they do not control. They share information and coordinate actions across boundaries. Traditional security approaches struggle in this setting because they were scoped to specific environments. A Zero Trust architecture can address these constraints. It offers a security approach that fits distributed cloud-edge environments beyond the physical or digital perimeter. More importantly, it changes how organizations think about trust itself: from something assumed to something actively managed.

3.1 Why Traditional Security Models No Longer Work

For a long time, digital security followed a simple idea. Organizations protected their IT systems with a clear boundary. Once users or IT systems passed that boundary, they were considered trustworthy. Access rights often lasted for long periods. Internal networks were treated as secure spaces. This approach worked when IT environments were stable and centralized. Employees worked from fixed locations, applications ran in predictable settings, and external connections were limited.

[9] https://docs.gaia-x.eu/technical-committee/architecture-document/25.05/pdf/document.pdf

Such an approach is no longer appropriate. Organizations are using multiple cloud providers, shared services, and data. Employees and partners connect from many locations and devices. Machines and software systems interact automatically across companies and networks. Data moves constantly between cloud, edge, and on-premises systems.

In this environment, the idea of a clear “inside” and “outside” disappears. When trust is tied to location, one failure can expose large parts of the system. Long-lasting permissions do not reflect changing conditions. Security becomes fragile instead of resilient. These limits make traditional perimeter-based models unsuitable for federated and edge-driven ecosystems.[10]

3.2 What Zero Trust Really Means

Zero Trust starts with a different assumption: no interaction is trusted by default. Every request must justify itself. In simple terms, Zero Trust follows one rule: never trust automatically, always verify. This applies to people, machines, and software services alike.

Verification does not happen once at login. IT systems continuously check whether access still makes sense. Decisions consider who is requesting access, what they want to do, and under which conditions. Zero Trust does not care where a request comes from. Being “inside the network” offers no special privilege. What matters is whether the request can be justified at that moment. This shift turns security from a fixed setup into an ongoing process. Trust becomes something organizations actively establish and maintain.

3.3 How Zero Trust Differs from Classical Security Models

The difference between classical security and Zero Trust becomes clear when looking at how access decisions are made. Traditional models grant access based on location or prior approval. Once inside, users and IT systems often move freely. Security focuses on defending the boundary.

[10] https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-162.pdf

Zero Trust works step by step. Each interaction is evaluated on its own. Access is limited to what is needed for a specific task and a specific moment. Trust does not accumulate over time. This approach reduces risk. If an IT system fails or is compromised, its impact stays limited. It also increases transparency. Organizations can see why access is allowed or denied. Most importantly, Zero Trust scales better. It works even when IT systems, partners, and conditions change continuously.

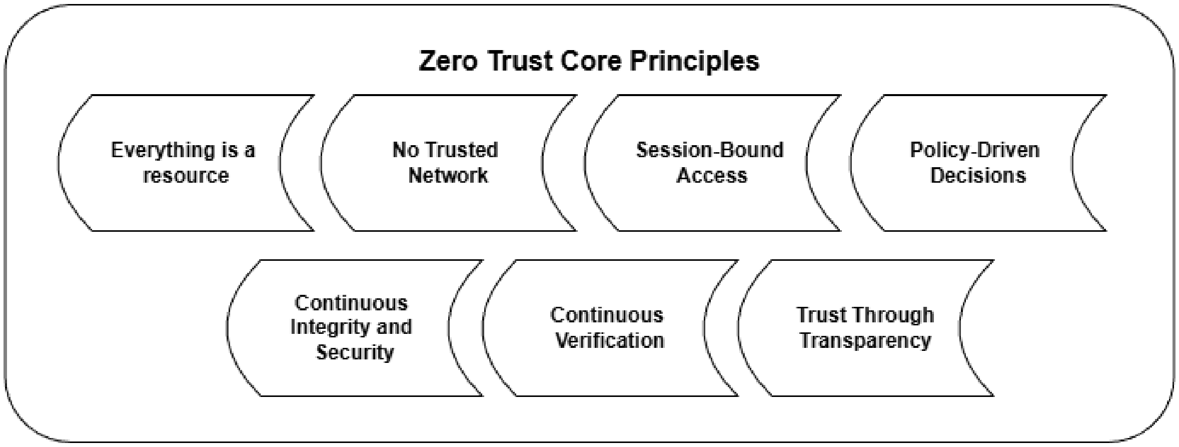

Figure 4 Zero Trust Principles.

3.4 What Zero Trust Changes for Organizations

Zero Trust is not just a technical adjustment. It changes how organizations manage responsibility and cooperation. Responsibility stays local. Each organization decides when and how others may access its IT systems and data. Zero Trust does not require handing control to a central authority. It supports independent decisions based on shared principles.

Security aligns more closely with business needs. Access decisions can reflect purpose, risk, and context. Organizations collaborate without opening their IT systems broadly or permanently. Zero Trust also strengthens resilience. Continuous verification allows IT systems to react to change. Permissions adjust when conditions shift. Problems remain contained instead of spreading. For leaders, this means greater flexibility without losing control. Zero Trust enables cooperation while preserving accountability and oversight.

3.5 Zero Trust as a Foundation for Federated Ecosystems

Federation connects independent IT systems without central control. This makes trust essential and challenging. Participants cannot rely on shared infrastructure or long-standing assumptions. Zero Trust provides the operating principle that makes federation work. Each participant verifies interactions independently while following shared expectations. Trust emerges through consistent verification, not through ownership or hierarchy.

In this way, Zero Trust turns federation from a structural idea into a practical reality. It enables secure cooperation across organizations, providers, and borders. The next chapter shows how this combination of federation and Zero Trust plays out in real cloud-edge environments, and how trust can work without central authority.

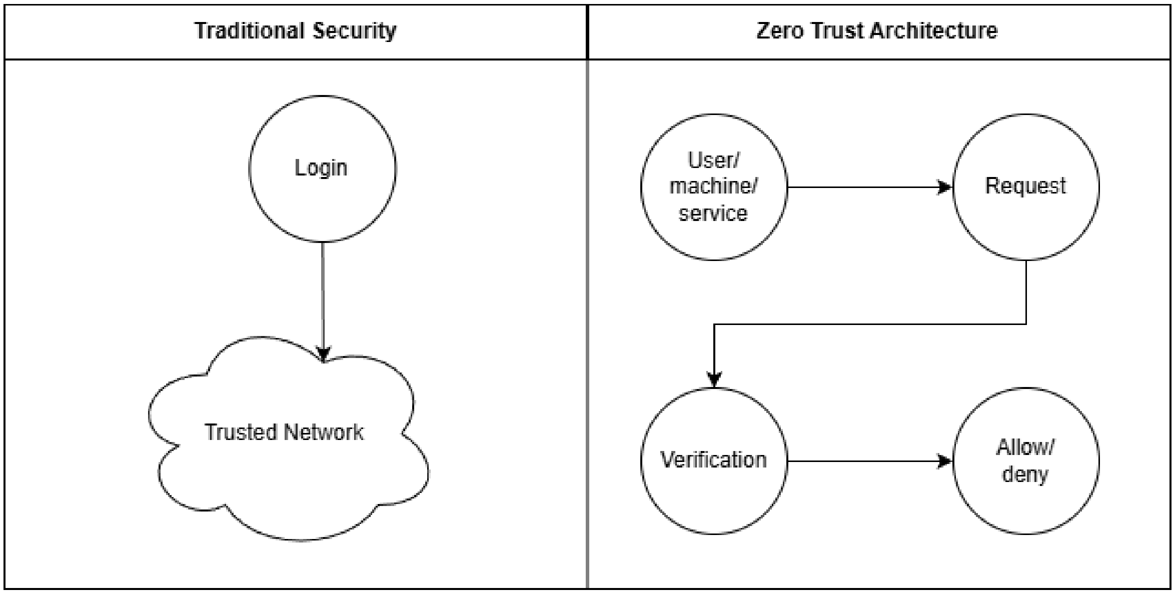

Figure 5 Traditional Security vs. Zero Trust architecture.

4. Zero Trust in Federated Digital Ecosystems

Federated digital ecosystems connect organizations that remain independent but need to work together. Each participant operates its own IT systems, follows its own governance rules, and remains accountable for its own decisions. There is no shared infrastructure that everyone controls and no central authority that can be trusted by default. As described in Chapter 3, this reality challenges traditional security models. In federated settings, cooperation is required, but trust cannot be assumed. Zero Trust provides the operating principle that allows collaboration to remain reliable without central control.

4.1 Secure Collaboration Without Central Trust

As explained in Chapter 3, Zero Trust shifts trust decisions to the moment of interaction. In a federated ecosystem, this shift is essential. Trust cannot be delegated to a single platform or provider. Each organization must decide independently whether an interaction is acceptable, while cooperation must still follow predictable rules.

Zero Trust supports this balance. Each participant applies its own trust decisions locally, while shared principles ensure that interactions remain consistent across the ecosystem. Organizations do not need to merge IT systems or align internal processes. What matters is that interactions follow the same logic of verification, which is achieved through machine-readable policies and standardized trust anchors. This approach enables collaboration across borders, sectors, and providers – without sacrificing sovereignty or autonomy.

4.2 Managing Identity and Access Across Independent Partners

Reliable cooperation depends on the ability to recognize interaction partners. In federated ecosystems, identity becomes the foundation for every trust decision. Zero Trust treats identity as something that must be confirmed whenever access is requested – not something that is assumed once and reused indefinitely. This applies equally to people, organizations, and automated IT systems.

Each participant manages identities within their own environment. Federation does not require shared user directories or a central identity provider.[11] What matters is that identity can be verified at the moment of interaction. Access decisions follow the same principle. They depend on purpose and context rather than on permanent permissions. This allows organizations to cooperate without exposing internal structures or granting broad, long-lasting access.[12]

In practice, this model builds on self-managed digital identities, verifiable credentials, and wallets for humans and machines.[13] These mechanisms support purpose limitation and minimal disclosure across organizational boundaries.

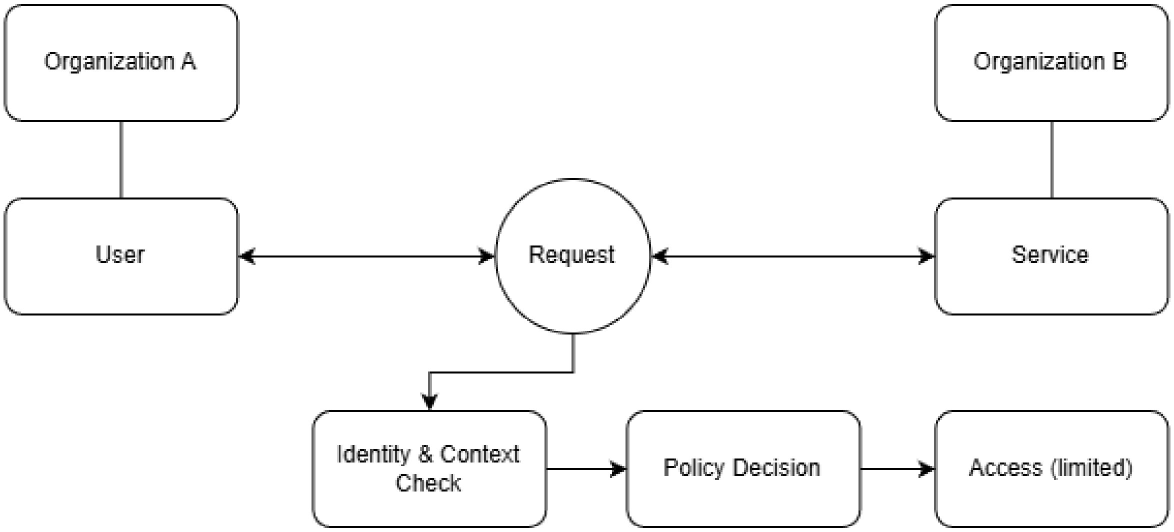

Figure 6 Requesting Access in Federation.

[11] https://openid.net/sg/openid4vc/

[12] https://www.w3.org/TR/vc-data-model/

[13] https://www.w3.org/TR/did-core/

4.3 Trust as a Chain, Not a Boundary

In federated ecosystems, trust rarely depends on a single factor. An interaction may need to meet legal requirements, contractual obligations, and operational constraints at the same time. A simple security boundary cannot capture this complexity.

Zero Trust replaces boundaries with a chain of verifiable elements. Identity confirms who is making a request. Integrity confirms that systems and services behave as expected. Rules define under which conditions access is allowed.

These elements work together to support informed decisions without exposing internal systems. Only the information required to justify the interaction is shared. Trust travels with the interaction rather than remaining tied to a network location. This model enables cooperation even when IT systems operate in different environments, under different providers, and across jurisdictions.

4.4 Data Sovereignty With Interoperability

Organizations must control how their systems, services, processes, and data are used, especially in regulated or sensitive domains. At the same time, collaboration often requires others to access results or insights.[14]

Zero Trust supports this balance by separating access from ownership. Data does not need to be copied or centralized to be useful. Access is granted for a specific purpose and under clearly defined conditions. Each interaction can be verified, limited, and revoked if conditions or policies change. This keeps data use transparent and accountable while enabling cooperation across organizational boundaries.

[14] https://eur-lex.europa.eu/eli/reg/2024/1183/oj/eng

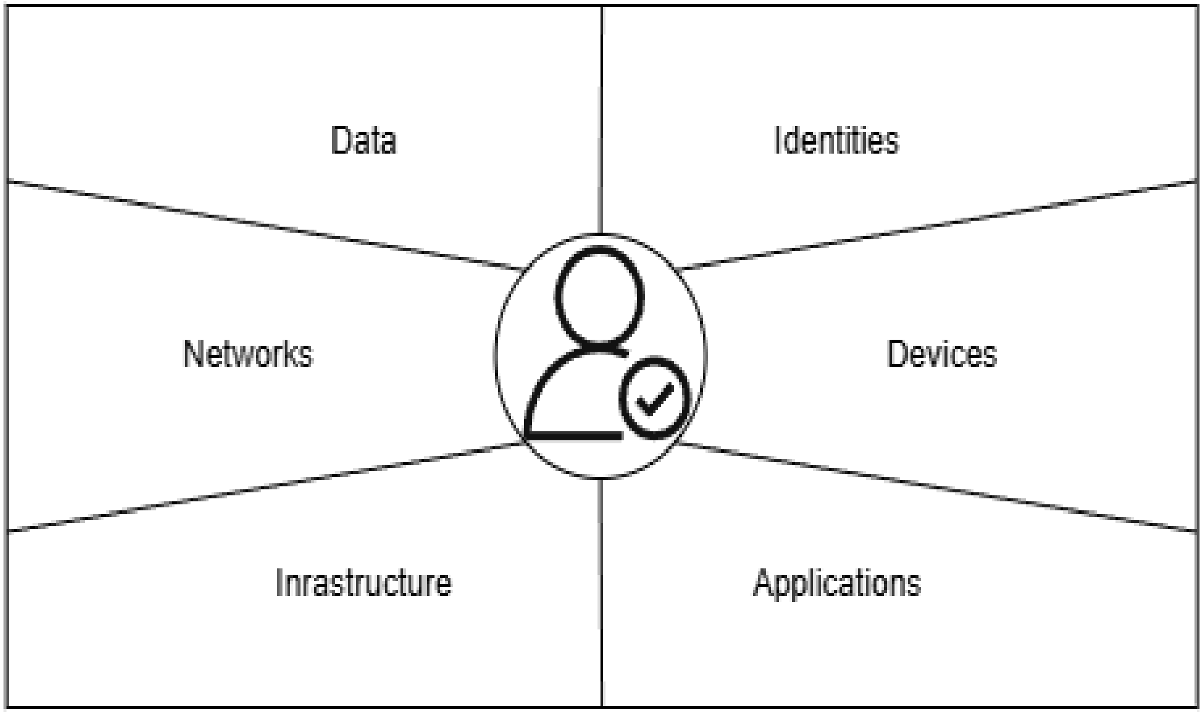

Figure 7 Access to different use cases.

4.5 Why Zero Trust Makes Federation Scalable

Federation delivers value as ecosystems grow. New participants join. Existing participants change technologies or providers. Without a consistent trust model, complexity quickly increases.

Zero Trust makes federation scalable by standardizing how trust decisions are made. Each interaction follows the same verification logic, regardless of who is involved. This consistency reduces friction and uncertainty. As a result, federated ecosystems can expand without redesigning trust relationships each time. Organizations remain autonomous, while cooperation stays reliable and predictable.

5. Zero Trust in Cloud-Edge Environments

Digital ecosystems no longer operate from a single location. Data is increasingly created and processed close to where events occur. Machines act on factory floors. Vehicles make decisions while moving. Medical devices and local systems operate independently and often in real time. This shift toward the edge changes how collaboration works – and how trust must be governed. As described in the previous chapters, federation and Zero Trust provide the foundation for cooperation across independent IT systems. Cloud-edge environments make this foundation essential.

5.1 What the Cloud-Edge Ecosystem Really Is

Edge environments bring computing closer to where data is generated. Instead of sending all information to centralized platforms, IT systems process data locally when speed, reliability, or control matter. Most organizations now operate across three layers at the same time. Cloud services provide scale and flexibility. On-premises IT systems maintain control in sensitive or regulated contexts. Edge IT systems connect the two by enabling fast, local decisions.

Together, these layers form a coherent cloud-to-edge landscape. Workloads and data move between them depending on context and need. No single layer replaces the others. Effective collaboration depends on all of them working together reliably, even when they are operated by different organizations.

5.2 Why Edge Environments Intensify the Trust Challenge

Cloud-edge environments are dynamic by nature. Devices connect and disconnect. Network conditions change. IT systems move across locations. High mobility and decentralized nodes create significant latency. Many edge devices also suffer from intermittent connectivity. Many decisions must be made immediately.

At the same time, granting broad or permanent trust is not an option. Edge IT systems often act autonomously and interact across organizational boundaries. Trust decisions must therefore balance autonomy with control. Zero Trust addresses this challenge directly. As outlined in Chapters 3 and 4, it verifies each interaction based on current conditions. This allows trust decisions to be made locally while still following shared principles across the ecosystem.

5.3 Humans, Machines, and Automated Interactions

Cloud-edge ecosystems rely heavily on automation. Machines and software services exchange information continuously, often without human involvement. These interactions must remain trustworthy, even when they happen at high speed and across boundaries. Zero Trust applies the same logic to machines as to people. Each interaction must justify itself. Identity and purpose matter, regardless of whether a human is involved.

For human users, this model supports mobility and flexibility. Access depends on context and intent, not on fixed locations or devices. Organizations can enable collaboration without weakening control. For machines and services, identity and integrity play a central role. Devices and workloads can prove who they are and that they operate as expected, supporting trustworthy interaction even in autonomous edge environments.

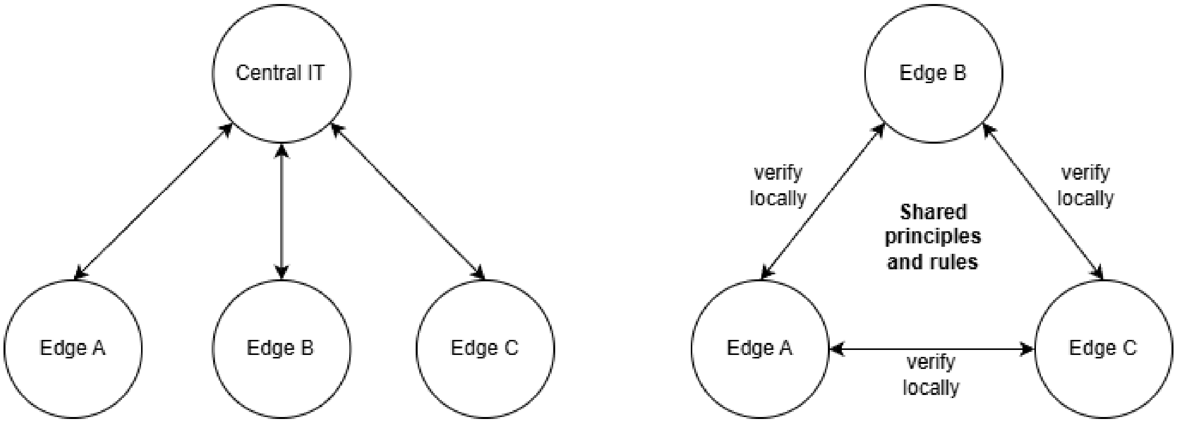

Figure 8 Centralized vs. Federated Ecosystems.

5.4 Data Sovereignty at the Edge

Edge environments strengthen a broader principle of sovereignty: systems should remain locally controlled where decisions are made. Legal, operational, and regulatory constraints often require that not only data, but also processes and services stay close to their point of execution.

Zero Trust supports this model by enabling controlled participation without relocation. Organizations can contribute results, services, or operational outcomes to shared processes without handing over control of their systems or environments. Each interaction is verified at the moment it occurs and limited to a defined purpose.

In federated cloud-edge ecosystems, this allows collaboration without centralization. Participants remain responsible for their systems while still taking part in joint operations. The result is a model that supports innovation and real-time cooperation while preserving accountability and trust.

5.5 Why Zero Trust Fits the Cloud-Edge Reality

Cloud-edge ecosystems combine movement, autonomy, and scale. Trust models must work across locations, providers, and technologies. They must support local decision-making without creating blind spots. Zero Trust fits this reality because it does not depend on fixed structures or central enforcement. Trust is verified at the point of interaction. Decisions can be made locally while following consistent rules across the ecosystem.

As cloud-edge environments continue to expand, Zero Trust becomes a necessity rather than an option. It enables secure operation where IT systems act independently but must still work together reliably. This makes Zero Trust a natural foundation for cloud-edge ecosystems and a key enabler for federation at scale.

6. From Principle to Practice: FACIS and the XFSC Tool Stack

Understanding federation and Zero Trust as concepts is important. For decision-makers, however, one question matters most: do these principles actually work in real organizations, under real constraints, and across real partners? FACIS addresses exactly this question. FACIS is part of the European 8ra initiative within the IPCEI-CIS framework. Its goal is not to build yet another platform or to centralize control. Instead, FACIS shows how organizations can work together in practice – based on shared principles, clear responsibilities, and verifiable trust.[15]

6.1 The Role of 8ra: framing the Cloud-to-Edge Landscape

8ra defines Europe's vision for a coherent cloud-to-edge landscape. It connects cloud services, local IT systems, and edge environments into one operational reality. This reflects how digital services are delivered today: distributed, dynamic, and often cross-border. Rather than promoting a single solution, 8ra sets a common direction. It emphasizes openness, interoperability, and sovereignty.

This vision creates the strategic context for federation and Zero Trust. A cloud-to-edge landscape only works when organizations can trust each other across independent IT systems and providers – without handing over control.[16]

[15] https://www.8ra.com/projects/facis/

[16] https://www.8ra.com/

6.2 What FACIS Contributes

FACIS turns this vision into a practical solution organizations can actually use. It focuses on how independent actors can collaborate securely without centralizing data or decision-making. FACIS does not replace existing IT systems. It connects them.

At its core, FACIS provides practical patterns for federation. These patterns describe how organizations join a shared ecosystem, how interactions are governed, and how trust is established. They serve as reusable blueprints rather than rigid rules. FACIS also tackles governance questions that often slow cooperation. Who is responsible for what? How are agreements enforced? How can compliance be demonstrated across organizational boundaries? By addressing these questions upfront, FACIS reduces uncertainty and makes collaboration easier to manage.[17]

6.3 Zero Trust as a Baseline Requirement

Within FACIS, Zero Trust is not an optional security add-on. It is a baseline architectural requirement that applies to every interaction across the federation. FACIS does not assume trust based on location, role, or prior relationships. Instead, access decisions are made when needed, based on identity, purpose, and context.

By anchoring Zero Trust at the architectural level, FACIS ensures consistency as ecosystems evolve. New participants can join securely, existing ones can adapt, and cooperation remains reliable over time. This turns Zero Trust into an enabler for scalable collaboration – supporting flexibility without sacrificing control.

6.4 The XFSC Tool Stack as an Enabler

The XFSC open-source tool stack provides the technical foundation that supports FACIS. Its components cover essential aspects of collaboration, such as onboarding participants,

[17] https://www.facis.eu/results/proof-of-concept-projects/

describing services, enforcing rules, and supporting trusted interactions.[18] From a management perspective, the individual tools matter less than their combined effect.

Together, they enable interactions that can be checked, governed, and repeated across organizations. Zero Trust principles apply across the entire stack. Trust decisions do not sit in one place. They shape how all components work together. This keeps federated ecosystems reliable even as complexity increases.[19]

6.5 FACIS as a Practical Showcase

FACIS proves its approach through concrete proof-of-concept scenarios in industrial and regulated environments. These scenarios show how federation and Zero Trust function under real operational and legal conditions.

They demonstrate that organizations can collaborate securely without centralizing data. They also show that Zero Trust does not slow down operations when it is built into processes from the start. By linking strategy, architecture, and practice, FACIS bridges vision and execution. It turns abstract principles into workable models that organizations can adapt to their own needs.

6.6 Purpose of XFSC in a Zero Trust Federation

The following section provides a reference view for architects and implementation teams. Decision-makers may treat it as a supporting illustration of how Zero Trust operates in practice.

XFSC does not act as a security product or a centralized control system. Its purpose is different. XFSC provides the operational backbone that allows Zero Trust principles to work across independent organizations, infrastructures, and environments.

[18] https://github.com/eclipse-xfsc/docs

[19] https://www.gxfs.eu/de/spezifikationsphase-1/

In a federated ecosystem, Zero Trust cannot be implemented as a single component. It must shape how identities are verified, how policies are evaluated, and how access is enforced – consistently and across organizational boundaries. XFSC supports this by embedding Zero Trust as a cross-cutting principle rather than isolating it in one module.

This means that Zero Trust is not "added" to federation. It is built into how federation operates. XFSC enables this by coordinating trust-relevant decisions while allowing each participant to remain autonomous.

6.6.1 Reference Architecture: Zero Trust in a Federated Cloud-Edge Ecosystem

The reference architecture illustrates how Zero Trust operates in a federated cloud-edge environment. Each organization runs its own infrastructure and remains responsible for its own systems. Cloud, edge, and on-prem environments coexist and interact depending on operational needs.

XFSC components do not replace these environments. Instead, they provide a shared framework that enables trustworthy interaction between them. Trust decisions are made where interactions occur, not in a central location. This architecture shows how federation scales without centralization. Organizations can join or evolve independently while following a common trust logic.

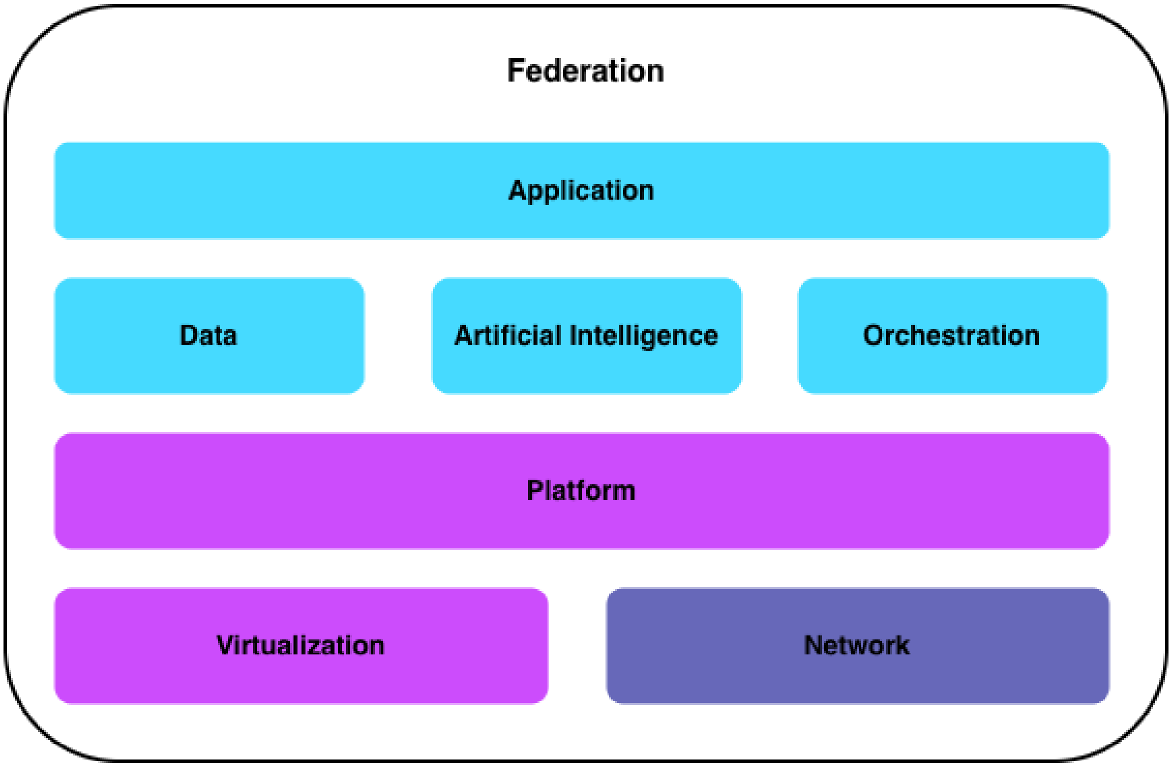

Figure 9 Federation Architecture.

6.6.2 Identity, Policy, and Access as a Continuous Trust Flow

In a Zero Trust federation, trust does not exist as a static state. It flows through every interaction. First, identity is verified. Participants – whether people, machines, or services – prove who they are using verifiable means. This verification does not rely on long-term assumptions.

Next, policies determine whether an interaction is allowed. These policies reflect purpose, context, and agreed constraints. They ensure that access aligns with business intent and governance requirements.

Access is then enforced in a limited and time-bound way. Permissions apply only to what is needed and only for as long as conditions remain valid. Finally, trust is continuously reassessed. If conditions change, access can adapt or stop. This flow turns Zero Trust into an ongoing operational process rather than a one-time decision.

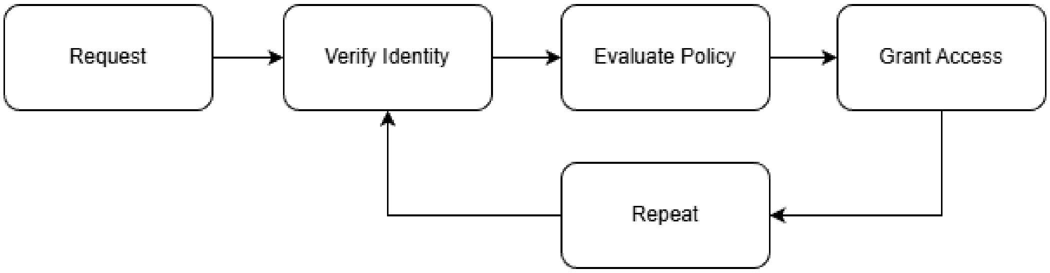

Figure 10 Zero Trust Interaction Flow.

6.6.3 Role of XFSC Components in Zero Trust Enforcement

Within this model, each XFSC component supports a specific trust function:

Table 1 XFSC Components and their Role – Zero Trust Model

XFSC Component	Role in the Zero Trust Model
OCM	Holds, presents and verifies identities on VC basis to provide verified data to subsystems
PCM	Provides holder capabilities to a natural user to present VCs via mobile or web
TSA	Policy enforcement and policy administration
AAS	AAS is an OIDC Bridge for authentication. The identity is anchored over TSA crypto provider, in combination via OCM
TRAIN	DNSSEC based discovery for trustworthy zones and their records behind it
Federated Catalogue	Acts as a digital "shop window" in a federated cloud-edge ecosystem, making trusted data and services visible without storing them centrally; enables organizations to collaborate securely and autonomously by allowing offers to be discovered and used under clearly defined rules

Together, these components ensure that trust decisions remain verifiable, distributed, and consistent – without requiring a central authority.[20]

6.6.4 Anchoring Zero Trust as a Baseline Architecture Requirement

Within FACIS and XFSC, Zero Trust is not optional. It acts as a baseline requirement for participation in a federated ecosystem. Organizations adopt Zero Trust as part of onboarding, governance, and daily operations. Trust rules become part of service agreements, compliance mechanisms, and audit processes. This ensures that security, governance, and accountability align from the start. By anchoring Zero Trust at this level, federated ecosystems remain robust as they grow. New participants integrate without weakening trust. Existing participants evolve without breaking cooperation.

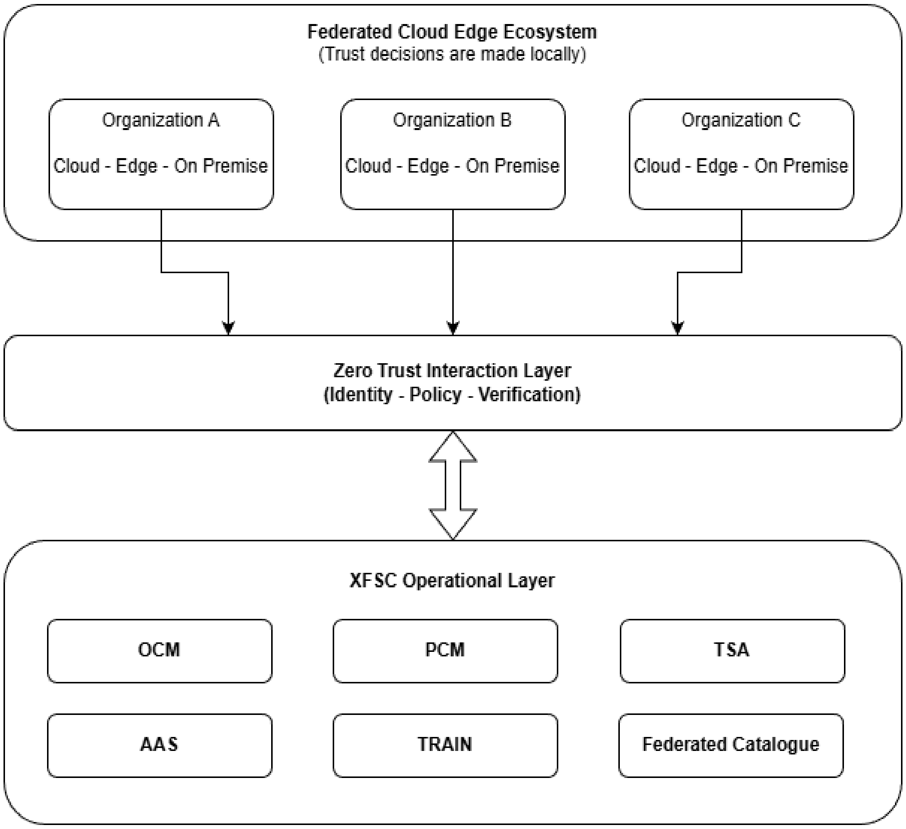
Federated Cloud Edge Ecosystem
(Trust decisions are made locally)
Organization A
Cloud - Edge - On Premise
Organization B
Cloud - Edge - On Premise
Organization C
Cloud - Edge - On Premise
Zero Trust Interaction Layer
(Identity - Policy - Verification)
XFSC Operational Layer
OCM
PCM
TSA
AAS
TRAIN
Federated Catalogue

Figure 11 Ecosystem layers.

[20] https://www.gxfs.eu/de/spezifikationsphase-2/

7. European and Global Standards Landscape

Federated digital ecosystems and Zero Trust do not start from scratch. They build on European and international standards that aim to make digital collaboration secure, reliable, and interoperable. Aligning with these standards matters, as it establishes credibility, legal certainty, and confidence for long-term adoption. Rather than adding new layers of rules, federation and Zero Trust bring existing principles together. They organize them into a model that fits today's distributed cloud-to-edge reality.

7.1 European Trust and Sovereignty Frameworks

To operationalize the principles of sovereignty and decentralized trust, the FACIS architecture aligns with established European frameworks. These initiatives provide the necessary legal and technical standards to make federated Zero Trust scalable.

The Gaia-X Trust Framework provides the technical basis for the "shared governance" required in federations. It ensures that autonomy and verifiable trust are not just abstract goals, but are implemented through transparent, machine-readable rules. By adopting Gaia-X principles, the FACIS architecture ensures that trust remains verifiable across all participants without requiring a central authority.

In parallel, eIDAS 2.0 (electronic IDentification, Authentication and Trust Services) and the European Digital Identity Wallet create a common foundation for trusted digital identities across Europe. They allow people and organizations to prove their identity in a reliable, standardized way. This is essential in federated environments, where partners must recognize and verify each other across borders.[21] Together, these frameworks promote ecosystems that remain open, sovereign, and interoperable. They support collaboration without forcing organizations into uniform technologies or centralized platforms.

[21] https://www.bundesdruckerei.de/de/innovation-hub/eidas/eidas-2-0

7.2 Zero Trust in International Guidance

Zero Trust is also anchored in international security guidance. The most prominent reference is the Zero Trust Architecture defined in NIST SP 800-207 (National Institute of Standards and Technology Special Publication). It describes a move away from perimeter-based security toward continuous verification of every interaction. This guidance focuses on principles, not products. It explains how organizations should make trust decisions dynamically, based on current conditions and context. This makes Zero Trust suitable for cloud, edge, and hybrid environments, and especially relevant for federated ecosystems.

European authorities support this direction. Publications from the German Federal Office for Information Security and from ENISA underline the limits of traditional security models. They highlight the need for continuous verification in distributed environments and frame Zero Trust as a strategic response to modern digital cooperation, not as a niche security concept.[22]

7.3 Standards for Identity and Controlled Data Exchange

Federated ecosystems depend on knowing who is involved and on controlling how information is shared. International standards for digital identities and secure data exchange are key here. Standards developed by the World Wide Web Consortium enable digital credentials that allow participants to prove certain facts or permissions without revealing more than necessary. This supports controlled sharing and helps organizations keep sensitive data under their own control.

Related standards define how such proofs can be presented and checked across organizational boundaries. They allow IT systems to rely on verified information instead of assumptions.[23] This makes cooperation predictable, scalable, and repeatable. By using open

[22] https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report%20-%20Digital%20Identity%20-%20Leveraging%20the%20SSI%20Concept%20to%20Build%20Trust.pdf

[23] https://norbert-pohlmann.com/wp-content/uploads/2022/05/SSI-White-Paper-EN-Prof-Norbert-Pohlmann.

standards, federated ecosystems avoid dependency on proprietary solutions. Interoperability becomes a built-in feature rather than a costly afterthought.

7.4 Why Standards Strengthen Federated Ecosystems

Standards do more than ensure compliance. They create a shared language and shared expectations. Organizations from different sectors and countries can cooperate even when their internal systems differ.

Aligning federation and Zero Trust with recognized standards builds trust among participants. It lowers entry barriers and reduces uncertainty for decision-makers. In this way, standards do not restrict innovation. They provide a stable foundation for open, sovereign, and scalable digital ecosystems to grow.

8. Industry Implications and Use Cases

The value of federated digital ecosystems and Zero Trust becomes clearest in practice. Across industries, organizations face similar pressures. They must work with many partners, protect sensitive information, and meet regulatory requirements. At the same time, they need speed, flexibility, and resilience to remain competitive. Federation and Zero Trust respond to these pressures in a practical way. They enable cooperation without central control and trust without blind reliance on long-standing relationships.

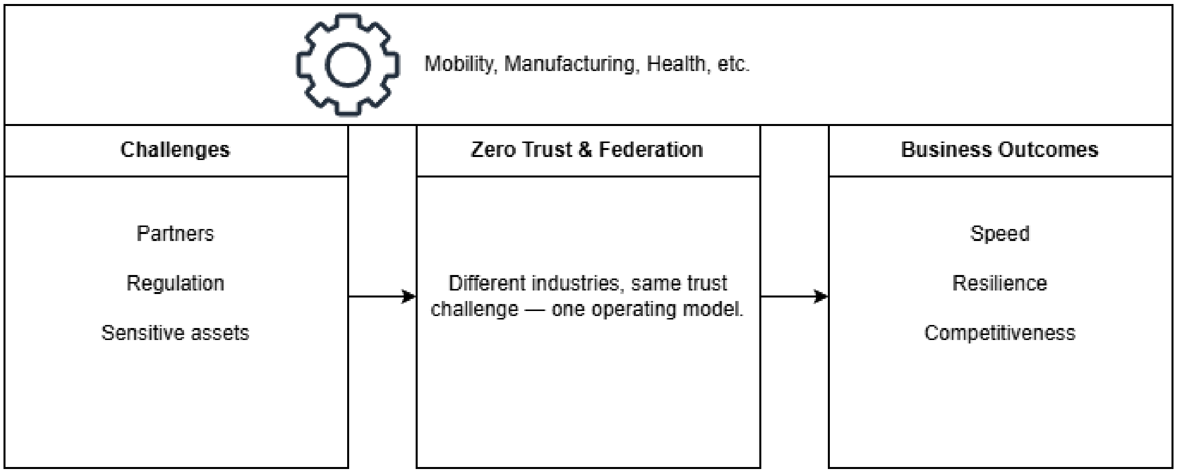

Figure 12 Outcomes with Zero Trust in Federation.

8.1 Mobility and Transportation Ecosystems

Modern mobility systems depend on constant coordination. Vehicle manufacturers, suppliers, infrastructure operators, service providers, and public authorities all play a role. Each actor runs its own IT systems and remains responsible for its own data and decisions.

In centralized environments, participants may hesitate to share sensitive operational information or to depend on a single coordinating entity. Changes in partners, providers, or regulations quickly increase complexity and cost.

A federated approach supported by Zero Trust offers a different path. Each participant retains control over its systems while participating in shared processes. Information is accessed only when needed and only for a specific purpose. Trust is created through verification, not through permanent access. This enables real-time coordination without centralizing data. Mobility services can scale across regions, adapt to change, and remain resilient even as ecosystems evolve.[24]

8.2 Manufacturing and Industrial Supply Chains

Manufacturing relies on highly distributed supply chains. Production involves many specialized partners, often spread across regions and countries. Effective coordination requires sharing schedules, status updates, and quality information across organizational boundaries.

At the same time, companies must protect intellectual property and competitive knowledge. Moving sensitive data into a shared platform can increase risk and weaken trust between partners.

Federation allows organizations to collaborate without giving up control. Each partner decides what information to share and under which conditions. Zero Trust ensures that access remains limited, transparent, and tied to a clear purpose.[25]

This approach strengthens supply-chain resilience. Organizations can onboard new partners faster, switch providers more easily, and respond to disruptions without rebuilding their entire digital landscape. Cooperation becomes more flexible and less dependent on fixed trust relationships.

8.3 Aerospace and Highly Regulated Environments

Aerospace and aviation environments demand especially high levels of trust and accountability. Manufacturers, operators, maintenance providers, regulators, and certification

[24] https://www.facis.eu/result/overview-aviation-federation/

[25] https://www.facis.eu/wp-content/uploads/2025/10/FACIS-PoC-1-Digital-Collaboration-by-Federation.pdf

bodies must coordinate closely. Data must be accurate, traceable, and handled in line with strict regulations.[26]

In such settings, trust cannot rely on informal agreements or permanent permissions. Every interaction must meet defined requirements. Zero Trust supports this by checking access decisions against current conditions and verified information.

Federation allows these actors to collaborate across organizational and national boundaries without centralizing control. Each participant remains accountable for their role while contributing to shared processes. Compliance becomes easier to demonstrate because interactions follow transparent and verifiable rules. This combination supports innovation while maintaining security, reliability, and regulatory confidence.

8.4 Common Patterns Across Industries

Across all these examples, the same pattern appears. Organizations need to collaborate, but they cannot rely on assumed trust or centralized control. They must remain autonomous while working within a larger ecosystem.

Federation provides the structure for this collaboration. Zero Trust provides the discipline that makes it reliable. Together, they allow ecosystems to grow across industries and borders without losing control.

These patterns extend far beyond the examples shown here. They apply wherever digital collaboration involves independent actors, sensitive information, and rapidly changing environments.

[26] https://www.facis.eu/wp-content/uploads/2025/10/Final-FACIS-Aviation-Federation-8ra-PoC-V1.0.pdf

9. Conclusion and Outlook

The shift toward distributed digital ecosystems marks a decisive phase for Europe's economy. As cloud, edge, and on-premises systems merge, secure collaboration becomes a strategic capability. **Federation** provides the structural model for this cooperation, while **Zero Trust** serves as the essential operating principle to ensure reliability without central control.

9.1 Synthesis: Trust as a Competitive Advantage

In the cloud-to-edge continuum, traditional security models are obsolete. Zero Trust enables local autonomy while applying consistent trust rules across distributed IT systems. This balance of interoperability and sovereignty aligns perfectly with European values of openness and accountability. Initiatives like FACIS demonstrate that this is no longer a theoretical concept, but a practical reality for sovereign digital ecosystems.

9.2 Strategic Action Plan

The transition to federated Zero Trust is a leadership decision. Stakeholders must take specific actions to ensure long-term competitiveness:

Table 2 Stakeholder Responsibility

Stakeholder	Core Responsibility
Industry Leaders	Treat Zero Trust as a governance topic; invest in scalable, decentralized architectures.
Cloud/Edge Providers	Design "Federated Trust by Default"; support open standards and customer data control.
Policymakers	Support interoperable trust frameworks; anchor Zero Trust in future regulations and funding.

9.3 Shaping the Digital Future

Looking ahead, competitiveness will be defined by the ability to collaborate without central control. Organizations that govern trust explicitly will move faster and adapt more easily to change. By embracing these principles, Europe can build resilient, sovereign, and scalable ecosystems where independent systems work together **by design, not by accident.** Ultimately, Federation and Zero Trust are choices about how our society and economy choose to collaborate.

References

[1] Ezhilmathi Krishnasamy, Sebastien Varrette, and Michael Mucciardi, 2020, Edge Computing: An Overview of Framework and Applications, https://prace-ri.eu/wp-content/uploads/Edge-Computing-An-Overview-of-Framework-and-Applications.pdf

[2] Mahadev Satyanarayanan, 2016, The Emergence of Edge Computing, https://elijah.cs.cmu.edu/DOCS/satya-edge2016.pdf

[3] Bharat Bhooshan Tyagi, 2024, Edge Computing: Everything You Need to Know, https://www.globallogic.com/wp-content/uploads/2024/04/edge-computing.pdf

[4] Bundesamt für Sicherheit in der Informationstechnik, 2023, Positionspapier Zero Trust 2023, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeLeitlinien/Zero-Trust/Zero-Trust_04072023.pdf

[5] National Institute of Standards and Technology, 2020, NIST Special Publication 800-207 Zero Trust Architecture, https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf

[6] Techconsult GmbH and Prof. Dr. Norbert Pohlmann, 2022, Security & digitale Identitäten in einer digitalisierten Welt, https://norbert-pohlmann.com/wp-content/uploads/2022/11/eco-studie_security-und-digitale-identitaeten-in-einer-digitalisierten-welt-prof-norbert-pohlmann.pdf

[7] Pierre Gronlier, 2024, An Introduction to the Gaia-X Trust Framework, https://gaia-x.eu/wp-content/uploads/2024/05/An-Introduction-to-the-Gaia-X-Trust-Framework_2024-V4.pdf

[8] National Institute of Standards and Technology, 2023, NIST Special Publication NIST SP 800-207A – A Zero Trust Architecture Model for Access Control in Cloud-Native Applications in Multi-Location Environments, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207A.pdf

[9] Gaia-X European Association for Data and Cloud AISBL, 2025, Gaia-X Architecture Document – 25.05 Release, https://docs.gaia-x.eu/technical-committee/architecture-document/25.05/pdf/document.pdf

[10] National Institute of Standards and Technology, 2014, NIST Special Publication 800-162 Guide to Attribute Based Access Control (ABAC) Definition and Considerations, https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-162.pdf

[11] OpenID Foundation, 2025, OpenID for Verifiable Credentials – Overview, https://openid.net/sg/openid4vc/

[12] World Wide Web Consortium, 2025, Verifiable Credentials Data Model v2.0, https://www.w3.org/TR/vc-data-model/

[13] World Wide Web Consortium, 2022, Decentralized Identifiers (DIDs) v1.0, https://www.w3.org/TR/did-core/

[14] European Union, 2024, Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework, https://eur-lex.europa.eu/eli/reg/2024/1183/oj/eng

[15] 8ra Cloud-Edge Continuum, 2025, FACIS, https://www.8ra.com/projects/facis/

[16] 8ra Cloud-Edge Continuum, 2025, Europe's Next Generation Cloud Infrastructure and Services, https://www.8ra.com/

[17] FACIS, eco – Association of the Internet Industry, 2025, Proof of Concepts, https://www.facis.eu/results/proof-of-concept-projects/

[18] Eclipse Foundation, 2025, XFSC Documentation, https://github.com/eclipse-xfsc/docs

[19] eco – Association of the Internet Industry, 2025, Spezifikationsphase 1, https://www.gxfs.eu/de/spezifikationsphase-1/

[20] eco – Association of the Internet Industry, 2025, Spezifikationsphase 2, https://www.gxfs.eu/de/spezifikationsphase-2/

[21] Bundesdruckerei GmbH, 2023, eIDAS 2.0: alle Änderungen im Überblick, https://www.bundesdruckerei.de/de/innovation-hub/eidas/eidas-2-0

[22] enisa – European Union Agency for Cybersecurity 2022, DIGITAL IDENTITY - Leveraging the Self-Sovereign Identity (SSI) Concept to Build Trust, https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report%20-%20Digital%20Identity%20-%20Leveraging%20the%20SSI%20Concept%20to%20Build%20Trust.pdf

[23] Berthold Maier and Prof. Dr. Norbert Pohlmann, 2022, Gaia-X secure and trustworthy ecosystems with Self Sovereign Identity, https://norbert-pohlmann.com/wp-content/uploads/2022/05/SSI-White-Paper-EN-Prof-Norbert-Pohlmann.pdf

[24] FACIS, eco – Association of the Internet Industry, 2025, Aviation Federation: Concept at a Glance, https://www.facis.eu/result/overview-aviation-federation/

[25] FACIS, eco – Association of the Internet Industry, 2025, Digital Collaboration by Federation, https://www.facis.eu/wp-content/uploads/2025/10/FACIS-PoC-1-Digital-Collaboration-by-Federation.pdf

[26] FACIS, eco – Association of the Internet Industry, 2025, Proof-of-Concept Specification for Digital Collaboration by Federation, https://www.facis.eu/wp-content/uploads/2025/10/Final-FACIS-Aviation-Federation-8ra-PoC-V1.0.pdf