Summary – Email Security and Digital Sovereignty: Opportunities through Your Own Domains and Top-Level Domains

On 19 November 2025, an expert panel discussion convened at the IPB Internet Provider in Berlin, on the topic of: “**Email Security and Digital Sovereignty**: **Opportunities through Your Own Domains and Top-Level Domains**”.

This event was hosted by ICANN Org and eco – Association of the Internet Industry. The discussion brought together leading voices from technology, business, and policy to explore how managing proprietary domains and top-level domains (TLDs) empowers digital sovereignty, strengthens security, and builds trust online.

The event was specifically moderated by **Thomas Rickert,** Director, Names & Numbers Forum of eco Association.

Speakers included:

- **Dr. Michael Littger,** Strategy Director, cyberintelligence.institute
- **Katrin Ohlmer,** Founder and Managing Director, DOTZON GmbH
- **André Görmer,** Head of the Email Competence Group, eco Association
- **Caroline Krohn,** Head of Digital Consumer Protection, German Federal Office for Information Security (BSI)
- **Christopher Mondini,** Vice President, Stakeholder Engagement & Managing Director Europe ICANN

19/11/2025
5:30 PM - 9:00 PM
IPB Internet Provider Berlin

Email Security and Digital Sovereignty: Opportunities through your own Domains and Top-Level Domains

ICANN · I/P/B/ Internet Provider Berlin · 30 eco

André Görmer
Head of the Email Competence Group
eco

Caroline Krohn
Head of Digital Consumer Protection
BSI

Katrin Ohlmer
CEO
dotBerlin & DOTZON

Christopher Mondini
Vice President, Stakeholder Engagement & Managing Director
ICANN

Dr. Michael Littger
Strategy Director
cyberintelligence.institute

Thomas Rickert
Director Names & Numbers
eco

Executive Overview

Leading experts from technology, business, and policy convened in Berlin to discuss the strategic opportunities offered by managing proprietary domains and top-level domains (TLDs). The panel explored how domain ownership enables digital sovereignty, reinforces cybersecurity, and builds trust in digital communications. Participants examined practical challenges and policy considerations for European organizations navigating a complex geopolitical and technological environment.

The discussion underscored that digital sovereignty is not only a political or legal concept but also an economic and technical imperative. Maintaining control over digital infrastructure, domain ownership, and email authentication protocols enables organizations to operate with independence while preserving trust, brand integrity, and resilience in their communications.

Defining Digital Sovereignty

Economic dimension

Dr. Michael Littger, Strategy Director of cyberintelligence.institute, framed digital sovereignty primarily as an economic issue centered on value creation. He argued that Europe's digital sovereignty should focus on retaining economic value within the continent rather than relying heavily on non-European providers. Using German data centers as an example, **Littger** highlighted that although billions are invested locally, much of the economic benefit flows to US chip manufacturers and software companies. Europe often only profits from hardware construction and operational staffing, while critical intellectual property and software revenues exit the region.

Freedom of choice and independence

Littger further emphasized that sovereignty also involves freedom of choice. Organizations must retain the ability to switch providers or services without experiencing catastrophic interruptions. Using Deutsche Bahn as an analogy, he illustrated responsible planning for critical dependencies, pointing out that the company maintains manual payroll processing plans in case their SAP (Systems, Applications, and Products in Data Processing) systems fail. He expressed concern over proposals for German public administration to rely entirely on Microsoft-operated cloud services, questioning why such dependencies are considered acceptable.

Control over services

Katrin Ohlmer, Founder and Managing Director of DOTZON GmbH, added that digital sovereignty encompasses the ability to determine which features and services to adopt rather than being limited by vendor-provided defaults. This extends to decisions regarding hypervisors, cloud services, software solutions, and TLD operators. She referenced initiatives like STACKIT's German cloud infrastructure as positive steps, while noting the digital ecosystem remains in flux.

The aim of this part of the discussion was not to provide a specific definition of digital sovereignty, but rather to offer an overview of the various dimensions currently being discussed under this topic.

Domains as a Pillar of Digital Resilience

The panel linked domain ownership directly to organizational sovereignty. **Dr. Michael Littger** noted that controlling proprietary domains strengthens independence across multiple dimensions. Organizations gain authority over communication channels, service endpoints, and the trust associated with their digital identity. Ownership allows firms to define their own security standards, implement SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail), and DMARC (Domain-based Message Authentication, Reporting, and Conformance) protocols, alongside control metadata, registrar procedures, and governance structures – critical tools for avoiding vendor lock-in.

Katrin Ohlmer illustrated these advantages with concrete examples. These included:

- **BNP Paribas (.bnpparibas):** The French bank reduced phishing attacks and improved customer trust by migrating to their proprietary TLD, despite the communication challenges involved in educating customers about the change.
- **Schwarz Group (.schwarz):** Operating both Lidl supermarkets and major cloud services in Germany, the company simplified internal IT access and onboarding by using .schwarz exclusively for all internal systems. New employees can be granted access to all services and platforms under .schwarz, dramatically lowering security risks from phishing attempts.
- **Geographic TLDs (.nrw, .stockholm, .berlin):** These created trustworthy namespaces for public services and mitigated conflicts with private operators. Berlin avoided complications that arose from a lawsuit between the city and the private operator of berlin.com by establishing clear official communication under .berlin.

Email Security and Authentication Standards

André Görmer, Head of the Email Competence Group at eco Association, highlighted the evolution from IP-based email security to domain-based authentication, explaining why domain control is increasingly critical. While owning a TLD provides operational control, successful email delivery depends on recognition and trust by receiving mail servers. He noted that some TLDs face deliverability challenges due to historical abuse, meaning messages may never reach recipients at major providers like GMX or Gmail.

Görmer stressed the importance of implementing authentication standards: SPF, DKIM, and DMARC. These protocols enable organizations to assert the legitimacy of their communications and ensure that recipients can reliably distinguish authentic messages from phishing attempts.

Thomas Rickert, Director, Names & Numbers Forum of eco Association, added context regarding TLD business models, emphasizing that open TLDs, while affordable and accessible to anyone, are more vulnerable to abuse. Even .com, despite being well-known and trusted, has the highest absolute number of abuse cases due to its popularity. In contrast, restricted or proprietary TLDs like .schwarz serve as trust anchors, allowing organizations to tell employees and the outside world that only communications under that TLD genuinely originate from the company.

The BSI Perspective on Pragmatic Security

Caroline Krohn, Head of Digital Consumer Protection of the German Federal Office for Information Security (BSI), offered a pragmatic lens, drawing attention to the limits of complete autonomy in a globalized ecosystem. The BSI's approach centers on control rather than isolation, focusing on negotiating technical safeguards and contractual protections to manage dependencies.

Krohn highlighted that dependencies exist universally – from US cloud providers to Chinese legislation – and that organizations must develop strategies to maximize sovereignty while operating globally. She illustrated this complexity with examples of German companies facing international pressures: Deutsche Telekom's CEO making controversial investment statements supporting US political figures, and SAP considering changes to diversity programs under American pressure. These examples demonstrate that sovereignty challenges transcend simple national boundaries.

She further compared the situation to German businesses operating in China, where companies encounter mandatory product backdoors, VPN restrictions, and other laws beyond Germany's influence. Similarly, Germans traveling to China must comply with Chinese legislation governing devices and data. The central question, she noted, is not whether to disengage entirely, but how to operate within these realities while maximizing control through technical measures and contractual safeguards.

Krohn stressed that honest assessment of dependencies and risks is more productive than ideological debates about autonomy, even though discussions of sovereignty can feel daunting amid geopolitical uncertainties.

The Sovereignty Debate: Pragmatism Versus Principle

A spirited debate emerged between those advocating for building European capacity and those supporting pragmatic approaches to existing dependencies. This exchange represented one of the most substantive discussions of the event.

Dr. Michael Littger argued that the status quo is unsatisfactory and worsening. He challenged what he called the “pragmatic” approach, citing the five billion euros Germany will pay to Oracle over the next five years and questioning why these massive sums aren’t redirected toward building European alternatives. He compared the situation to Europe’s former dependence on Russian oil, noting that industry lobbyists insisted oil would always flow until suddenly it didn’t. The same risk exists with digital dependencies, but the implications are more severe.

Littger referenced statements suggesting Deutsche Bahn might have only five months –or realistically five days – to migrate if disconnected from their cloud provider. Such scenarios, he argued, should disqualify those solutions entirely rather than merely prompting contingency planning. He took issue with what he perceived as relativism in arguments emphasizing global interconnection and avoiding market disruption, insisting that the core message must be about becoming more independent. While expressing no personal animosity toward American companies, **Littger** emphasized that competitive dynamics don't operate at the individual level, and Europeans must understand this reality.

Caroline Krohn countered that complete independence is unrealistic in a globalized world and that strategic safeguards represent a more achievable path forward. The BSI's approach focuses on what can be technically controlled and contractually protected rather than pursuing unattainable autonomy.

From the audience, **Klaus Landefeld** from eco Association and DE-CIX, emphasized the importance of first achieving sovereignty for European consumers and businesses, ensuring that data stays in Europe without foreign government access. He referenced President Macron’s legislative efforts to require European data storage and prohibit transfers to foreign governments, acknowledging this would be an uphill battle but necessary for establishing basic trust in European services.

ICANN’s Role in Internet Stability

Christopher Mondini, Vice President, Stakeholder Engagement & Managing Director Europe from ICANN, elaborated on ICANN’s neutral, multistakeholder model. ICANN serves as a global platform where governments, companies, and civil society actors collaboratively establish DNS policies. Even nations in conflict work together within ICANN working groups, fostering resilience through personal and institutional networks.

Mondini emphasized ICANN’s core contributions, including:

- Limited technical mandate prevents political or commercial capture.
- Collaboration with 188 governments through the Governmental Advisory Committee.
- Neutral DNS platform supports diverse global stakeholders.

Examples from Estonia and Armenia highlighted how digital infrastructure resilience enables continuity of services in geopolitically complex environments.

Thomas Rickert reinforced the importance of ICANN's deliberately limited mandate for preserving its integrity. When the Ukraine war began, ICANN received letters from both Ukrainian and Russian sides – Ukraine requesting suspension of the .ru domain, and Russia asking about Ukrainian ccTLD administration after potential absorption. ICANN has resisted numerous attempts to use it as a tool for content regulation, intellectual property enforcement, or political intervention. The organization's bylaws specifically prevent content regulation, and maintaining this restriction allows the DNS to function as a neutral platform where diverse businesses can operate.

Mondini also shared examples from his European region travels. He described landlocked Armenia in its difficult neighborhood and highly digitalized Estonia in its strategically complex location. Both countries demonstrate how communities in diverse circumstances develop solutions for resilience and sovereignty. These global discussions give him hope, and he noted that Europe remains the region where the most level-headed, thoughtful discussions about future directions occur among diverse sectors.

Technical and Operational Considerations

Katrin Ohlmer raised concerns regarding gaps in global TLD infrastructure. Only 70–75% of country-code TLDs worldwide have implemented DNSSEC, leaving notable gaps in countries such as Egypt, Bosnia-Herzegovina, Bolivia, Panama, Jamaica, and Nepal. Organizations operating internationally must consider these gaps when selecting TLDs to ensure consistent security standards. Proprietary TLDs or certain generic TLDs can mitigate these risks by providing predictable, standardized security features.

The panel also discussed practical governance considerations. These included:

- Clear succession planning and authentication for domain registration.
- Centralized oversight and anomaly detection.
- Brand integrity through consolidated TLD usage, e.g., Audi car dealers under .audi.
- Geographic TLDs for public recruitment platforms, establishing trust signals.

Practical Migration Strategies

Domain migration must be carefully managed. **André Görmer** and **Katrin Ohlmer** highlighted the need for both technical preparation and clear communication. Internally, employees should understand and champion the change. Externally, customers must be informed through newsletters, website notices, and reminders to update address books, for example. Technologies such as BIMI and services like Trusted Dialog in Germany provide verification tools, enhancing trust during migration.

An additional audience member introduced an often-overlooked element: control over the local part of email addresses (the portion before the @ sign). Assigning unique local parts to service providers allows automated filtering of unauthorized messages, providing an additional layer of security complementing domain-based authentication.

Responsibility, Awareness, and the Limits of Individual Action

Dr. Michael Littger raised questions about industry responsibility, initially using the metaphor of seatbelts: the industry installs seatbelts, but who fastens them? He argued that domain owners share responsibility for security, and the industry must help users understand their role in a safer Internet.

After ten years leading awareness campaigns, **Littger** acknowledged that awareness alone is insufficient. At a Diakonie Deutschland congress that morning, he observed frustration among the organization’s 700,000 employees over the lack of transparency in social media data handling. Organizations shouldn’t have to choose between using critical infrastructure and remaining ignorant of data practices. The burden cannot fall entirely on individual users or small organizations; instead, industry and policymakers must provide systems that ensure transparency and control by default, shifting security from an individual awareness issue to a systemic challenge.

Key Recommendations from Speakers

For businesses:

- Secure digital identity through second-level domains to enhance independence and portability.
- Consider proprietary TLDs (brandTLDs) for larger organizations to strengthen security, governance, and brand integrity.
- Implement SPF, DKIM, and DMARC as standard email authentication measures.
- Plan migrations with clear communication internally and externally.
- Audit dependencies to understand data locations and control.

For policymakers:

- Support European digital infrastructure to reduce reliance on foreign providers.
- Strengthen data sovereignty legislation to create trust frameworks.
- Promote portability rights under GDPR and the Data Act.

- Protect ICANN's independence to maintain a neutral global DNS platform.

For consumers:

- Use personal domains rather than provider-tied email addresses.
- Understand email authentication to verify sender authenticity.
- Support transparent services with clear data handling policies.

For the domain industry:

- Improve abuse mitigation and standardize security features, including DNSSEC.
- Increase transparency about TLD security and governance.
- Reduce barriers for organizations considering proprietary TLDs.

Looking Forward

Thomas Rickert emphasized actionable steps: individuals should use personal domains; businesses should view domains as foundational to digital identity; enterprises may benefit strategically from proprietary TLDs; policymakers can leverage GDPR and the Data Act to reinforce portability rights and reduce vendor lock-in.

Domain ownership provides a concrete, achievable path toward sovereignty, security, and resilience. Even simple second-level domain ownership provides vendor-agnostic identity. Individuals can use their own domains pointing to whatever email service they choose, and if preferences change, the domain can simply redirect elsewhere. The same principle applies at organizational scale – companies can use their own domains to maintain consistent identity while retaining freedom to change underlying platforms if terms of service become unacceptable.

These domain-based foundations for digital sovereignty complement other portability rights emerging through regulation. The GDPR's data portability provisions, combined with the Data Act's requirements, create historically favorable conditions for breaking free from provider lock-in. While migrating between vendors remains challenging, having stable digital identity and storefronts owned by the organization rather than the platform makes transitions feasible.

Resources and Next Steps

Participants were encouraged to explore:

- eco's Directory of new gTLD providers for the 2026 new gTLD program
- ICANN's 2026 new gTLD program
- eco's topDNS Initiative for DNS abuse mitigation resources and best practices

- The EUCRA (European Value Creation Alliance, Cybersecurity & Resilience) platform launched at the event for European collaboration (DE)
- BSI's initiative on securing email (DE)
- ICANN's multistakeholder processes for domain policy engagement