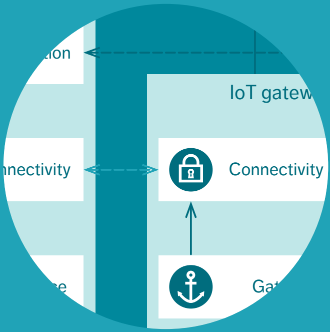
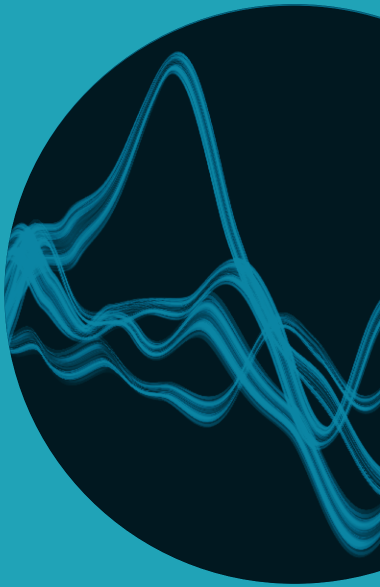
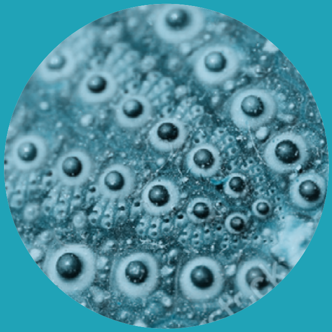
CHARTING THE FUTURE OF INNOVATION | #10·2017

ERICSSON TECHNOLOGY Review





END-TO-END IoT SECURITY



ERICSSON

END-TO-END Security Management FOR THE IoT

Industries everywhere are digitizing, which is creating a multitude of new security requirements for the Internet of Things (IoT). End-to-end (E2E) security management will be essential to ensuring security and privacy in the IoT, while simultaneously building strong identities and maintaining trust.

KEIJO MONONEN,
PATRIK TEPPO,
TIMO SUIHKO

As the diversity of IoT services and the number of connected devices continue to increase, the threats to IoT systems are changing and growing even faster.

■ To cope with these threats, the ICT industry needs a comprehensive IoT security and identity management solution that is able to manage and orchestrate the IoT components horizontally (from device to service and service user) and vertically (from hardware to application). In addition to this, the ability to address both security and identity from the IoT device all the way across the complete service life cycle will also be essential.

Figure 1 illustrates an E2E approach to security and identity that highlights three key aspects: security and identity management, security and identity functions, and trust anchoring.

IoT actors and trust

IoT systems support new business models that involve new actors in conjunction with traditional telecommunication services. Aside from consumers and mobile network operators, enterprises, verticals, partnerships, infrastructure, and services play increasingly vital roles. All of these actors affect trust.

Figure 2 presents the main and supporting IoT actors and their trust relationships. The three main actors in an IoT solution are the IoT service user,

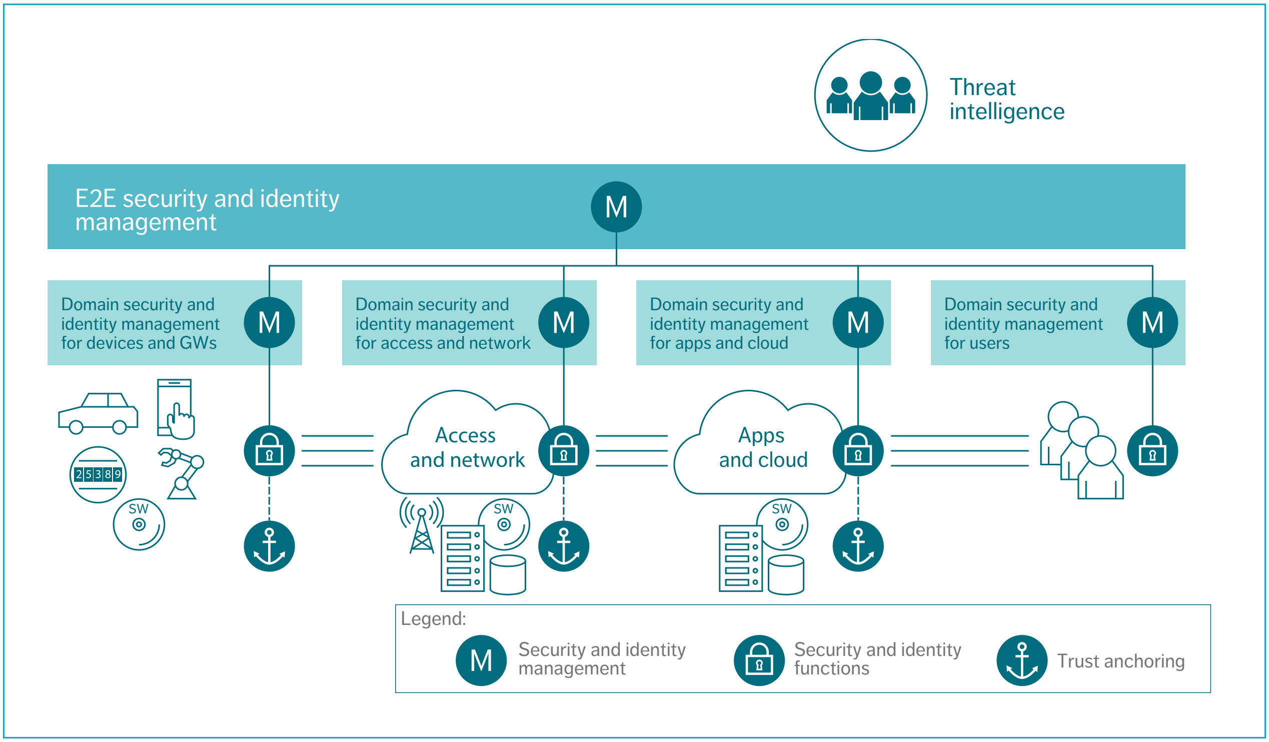

Threat intelligence
E2E security and identity management
M
Domain security and identity management for devices and GWs
Domain security and identity management for access and network
Domain security and identity management for apps and cloud
Domain security and identity management for users
25389
SW
Access and network
Apps and cloud
Legend:
Security and identity management
Security and identity functions
Trust anchoring

Figure 1 E2E approach to security and identity

the IoT service provider, and the devices that enable the provision of the IoT service. The supporting actors are the IoT platform service provider, whose role is to provide the IoT platform for the IoT service provider, and the connectivity service provider, whose role is to provide connectivity for the IoT devices and service.

The trustworthiness of services and service use depends on how the actors govern identities and data, security and privacy, and the degree to which they comply with the agreed policies and regulations. The combination of the security and identity functions is important for defining the trust level. For example, hardware-based trust does not help if the application does not make use of it. A fully trusted application does not help if the communication cannot be trusted. An E2E approach is therefore essential to ensure trust among all actors across the system.

E2E IoT security architecture

The purpose of an E2E IoT security architecture is to ensure the security and privacy of IoT services, protect the IoT system itself and prevent IoT devices from becoming a source of attacks – a Distributed Denial of Service (DDoS) attack, for example – against other systems.

Figure 3 illustrates Ericsson's view of how security can be managed and deployed in an E2E manner throughout IoT domains to monitor

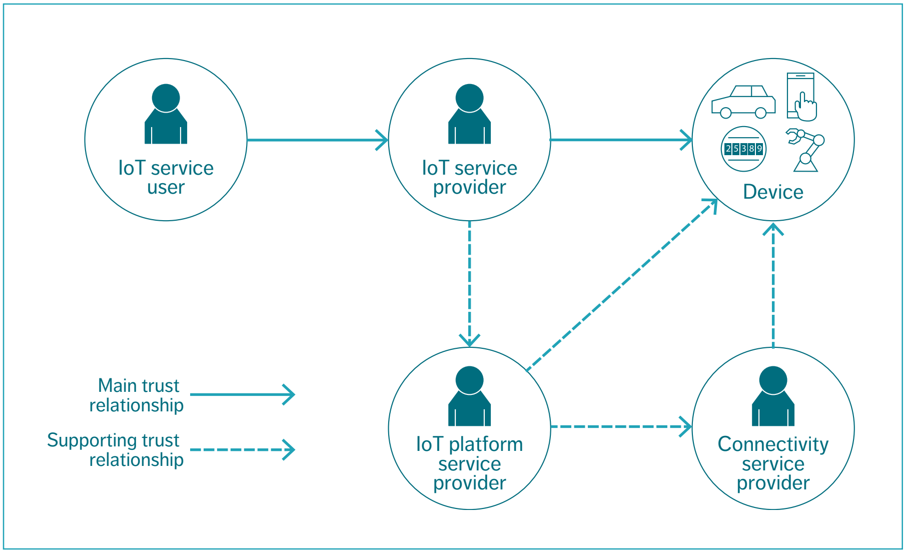

IoT service user
IoT service provider
Device
25389
Main trust relationship
Supporting trust relationship
IoT platform service provider
Connectivity service provider

Figure 2 The main and supporting IoT actors and their trust relationships

and protect system resources and assets. The architecture consists of an E2E security and identity management layer, domain (device, gateway, access, platform and application) specific management layers, and security and identity functions in each domain component.

An IoT system spans from the device via different network interfaces to the cloud that hosts the platform and applications that provide services that are consumed by IoT service users. Each element of the chain must be considered when designing an E2E approach to security and identity in the IoT.

This approach leverages advanced security analytics and machine learning to provide threat, risk and fraud management at both E2E and domain management layers. To meet industry security and privacy standards, an E2E security management solution must also be in charge of overall security and privacy policies and compliance and be able to coordinate across a multitude of domain management systems through the establishment of cross-domain identities and relevant policies. Domain management of security and identity functions within domains ensures that security and identities are properly managed, configured and monitored within the domain according to policies, regulations, and agreements. Vulnerability and security baseline management also occurs at the domain management layer based on E2E level policies.

According to this approach, the IoT service provider is responsible for managing IoT service security and identities E2E, whereas domain-level management can be delegated to the IoT platform service provider and connectivity service provider.

Figure 3 shows how the IoT domains are managed both horizontally and vertically. Horizontal (cross-domain) security is required at two levels: connectivity and application. Depending on connectivity type, security controls such as mutual authentication and encryption of data in transit are provided at the connectivity level. On top of connectivity, security is provided at the application level from device to cloud, based on identification and access management functions and application security policies. Application level security can be independent of or dependent on (federated with) the connectivity level security.

Vertical security from hardware to application can be used in every domain to provide hardware-based root of trust, ensuring the integrity of the domain. The domains are built on trusted hardware and software. When required by the industry and the use case, trust is anchored to hardware.

The domains include security and privacy functions to handle identity and access management, data protection and right to privacy, network security, logging, key and certificate management, and platform/infrastructure security (including virtualization security and hardware-based root of trust).

For critical IoT services, the level of security functions must be set high in accordance with the risk management results and service provider security policies. For less critical IoT services, a lower level may be sufficient.

Security policy and compliance management

Business-optimal and trust-centric IoT security is dependent on continuous risk management that balances criticality, cost, usability and effectiveness to fulfill different types of security Service Level Agreements in multi-tenant IoT systems. Since the current management of IoT security is spotty at best, it must be transformed into unified security management with adaptive protection, detection, response and compliance driven by security policies. Only in this environment can service providers and their customers leverage E2E network and application knowledge to secure assets across all contexts.

Our vision of security policy and compliance management defines security policies using industry standards, regulation and organizational policies. This approach helps to automate security and privacy controls, maintain them at a desired level even in a changing threat landscape, and shorten the reaction time in response to potential breaches. Real-time visibility regarding general and industry-specific security standards and regulations makes it possible for IoT service providers to remediate policy violations quickly and demonstrate compliance to security frameworks, including ISO, NIST, CSA, GDPR and CIS benchmarks, as well as an enterprise's own security and privacy policies. Having the security baseline configuration and compliance function at domain level ensures the automated hardening of the protected assets and supports continuous compliance monitoring in the defined security baseline.

> “ A HIGH DEGREE OF AUTOMATION IS NECESSARY TO ENSURE A SWIFT RESPONSE TO ANY IDENTIFIED THREATS AND ANOMALIES ”

Domain level security management requires an accurate asset inventory including all the assets that must be protected in the managed domain, such as authorized IoT devices and software. Automation of asset discovery and continuous monitoring is essential to keep the asset inventory updated. The vulnerability information is also correlated with the asset inventory to monitor and remediate the vulnerabilities of protected assets.

Rapid detection of attacks is crucial. Security monitoring and analytics functionalities must have the ability to analyze logs, events and data from IoT domain components combined with external data about threats and vulnerabilities. Machine learning technology makes it possible to learn from and make predictions based on data. Coupling a machine learning analytics engine with central threat intelligence improves the detection of zero day attacks and reduces the response time for known threats.

On top of a monitoring and analytics engine, solutions relating to vulnerability, threat, fraud and risk management, along with security policy and orchestration components, are also required to automate security controls and maintain them at desired levels in a changing threat landscape.

Combining the information feeds for vulnerability, threat and fraud management results in timely

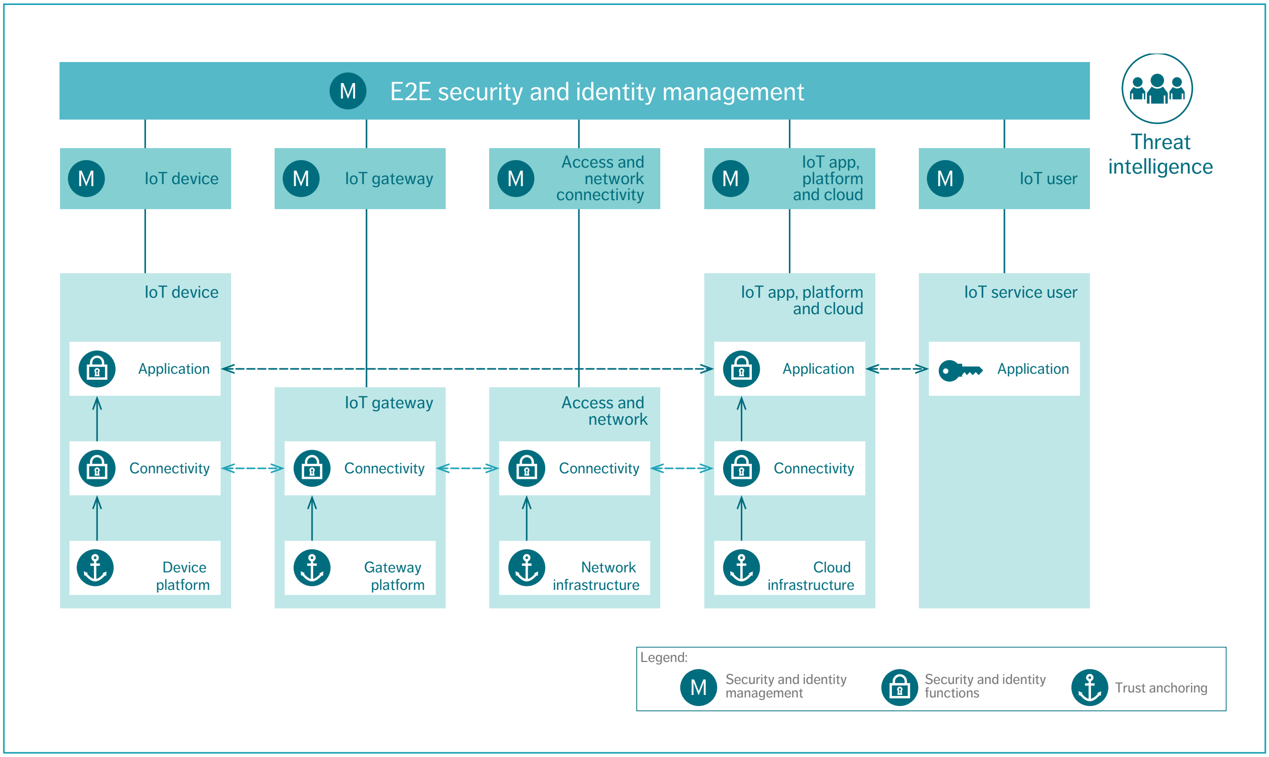


Figure 3 E2E approach to security and identity

and accurate information for evaluating potential risks and helps to direct efforts in protecting the most exposed critical assets. A high degree of automation is necessary to ensure a swift response to any identified threats and anomalies.

Since not all security breaches and attacks can be prevented, it is crucial to have an efficient security incident management process that ensures rapid response and recovery. Real-time insights and audit trails from tools such as security monitoring, analytics and log management help to find the root cause of an incident. The same information can be also used as the evidence in digital forensic investigations.

Identity management

The main purpose of identity management is to manage the life cycle of identities and provide identification, authentication and access control services for identities. There are various identities that serve different purposes in the IoT approach, but the main ones are for device and user identification. The others are used for management of devices, functions and services. Identifiers and keys are also used to sign data, including software and firmware. These different device identities are needed to identify the devices for connectivity within the access and network domains, and to identify device applications in the IoT platform and cloud domain.

The level of trust in the device identity depends on the strength of authentication both at the connectivity (for example, 3GPP, Wi-Fi and fixed) and application layers. For device identity to be trusted, strong authentication and follow-up of the device integrity – with the help of hardware-based root of trust in the device, for example – would be needed.

A device will have different identifiers depending on where it is in its life cycle. Life cycle management of device identities is part of the security management layer. More than one security management domain is involved when provisioning identities. Connectivity and IoT service provider could be different players where each player takes care of its own identity life cycle management.

When a device is manufactured, the vendor will give it an identifier that could have different trust levels. Vendor credentials could be protected in hardware (preferred) or they could be nothing more than a serial number printed on the device. The device has to be authenticated by the IoT system, and newly given identifiers and credentials (bootstrap process) will be used for connectivity and application accesses.

Identifiers and credentials can be changed during the device life cycle depending on different triggers such as expiration of credentials, change of service provider and so on. Connectivity identities are dependent on the connectivity type and have different life cycle management processes. For example, 3GPP access is based on SIM identities (IMSI and AKA credentials). SIMs are either physically removable ones or SIMs (i.e. eUICC) that can be remotely provisioned [1].

The user identities are needed to identify the users of the services within the applications and cloud domain. There may be several different ways to verify (authenticate) the user identities such as single- or multi-factor authentication, federated authentication, or authentication tokens. Each of these provides a certain level of authentication strength.

Due to layered security management architecture and the involvement of several actors (including industries) in the IoT, any identity and access management solution must be able to cooperate with and adapt to external identity and access management systems. On top of identification and authentication, there must also be access control for users so that only the permitted services are authorized.

Threat intelligence

Threat intelligence is built and shared in communities. Therefore, a centralized threat intelligence solution must be able to interface with different threat intelligence sources to learn about existing and new threats. Consolidation and correlation of security audit feeds from different domains are necessary to provide a clear view of threat insights across all IoT domains.

Automation and machine learning can be used to great advantage in threat intelligence, to create and share indicators of compromise that are actionable, timely, accurate and relevant to support strategic decision-making and to understand business risks in detail. Targeted threat intelligence feeds are a great way to generate customer-specific threat intelligence.

Two IoT use cases

Two concrete examples of how an E2E security management solution can help address IoT challenges are provided below.

DDoS detection and prevention

In October 2016, the Mirai botnet exploited a vulnerability in IoT devices to launch a DDoS attack against a critical DNS server that disrupted a number of the internet's biggest websites, including PayPal, Spotify and Twitter.

Mirai was designed to exploit the security weaknesses of many IoT devices. It continuously scans for IoT devices that are accessible over the internet and are protected by factory default or hardcoded user names and passwords. When it finds them, Mirai infects the devices with malware that forces them to report to a central control server, turning them into bots that can be used in DDoS attacks.

Strong detection and prevention mechanisms are needed against DDoS attacks that attempt to saturate the network by exhausting the bandwidth capacity of the attacked site, the server resources or service availability. In our view, an optimal outbound DDoS (botnet) detection and mitigation solution includes remote attestation to verify device trustworthiness and detect malware, monitoring of outbound traffic, anomaly detection, infected entities isolation or blocking and setting of traffic limit policies. Optimal inbound DDoS detection and mitigation includes monitoring of inbound traffic, anomaly detection, setting of traffic limit policies and redirecting malicious traffic to a botnet sinkhole.

The security management layer plays a critical role in detecting and mitigating DDoS attacks. In our framework, DDoS attacks are detected by the security monitoring and analytics functions through the observation of device and network behavior and identification of anomalies. Once an anomaly is detected, immediate mitigation actions can be triggered.

GDPR compliance

There is a legitimate expectation in society that IoT solutions will be designed with privacy in mind. This is becoming especially evident in certain jurisdictions: for example, in the European Union with the new General Data Protection Regulation (GDPR) [2].

Data integrity, data confidentiality, accountability and privacy by design are all fundamental to the protection of sensitive personal data. Such data can be protected via appropriate privacy controls. These controls include personal data identification and classification, personal data management and fair data processing practices. When actual personal data might be exposed, additional privacy protective measures will be applied such as data encryption and data anonymization.

Another focus area in the IoT security domain is the privacy breach response. Dedicated privacy logging and audit trail functionality can be used to improve the ability to prevent, detect and respond to privacy breaches in a more prompt and flexible way. Such capabilities will be essential to respond to privacy breaches swiftly (within 72 hours, as prescribed by the GDPR).

Implementing a GDPR compliance tool in the security management layer makes it easier to meet GDPR requirements. To do its job right, it must be able to provide identification and classification of personal data, enforcement of data privacy policies according to the GDPR, demonstration of compliance to the GDPR, and detection, response and recovery from privacy incidents.

Conclusion

The IoT offers a wealth of new opportunities for service providers. Those who want to capitalize on them without taking undue risks need a security solution that provides continuous monitoring of threats, vulnerabilities, risks and compliance, along with automated remediation. Ericsson's E2E IoT security and identity management architecture is designed with this in mind, managing and orchestrating the IoT domains both horizontally and vertically, and addressing both security and identity from the IoT device throughout the service life cycle. ✪

Terms and abbreviations

AKA – Authentication and Key Agreement | **CIS** – Center for Internet Security | **CSA** – Cloud Security Alliance | **DDoS** – Distributed Denial of Service | **DNS** – Domain Name System | **E2E** – end-to-end | **eUICC** – embedded Universal Integrated Circuit Card | **GDPR** – General Data Protection Regulation | **GW** – gateway | **IMSI** – International Mobile Subscriber Identity | **IoT** – Internet of Things | **ISO** – International Organization for Standardization | **NIST** – National Institute of Standards and Technology | **SIM** – Subscriber Identity Module | **SW** – software

THE AUTHORS

Keijo Mononen

◆ is general manager of Security Solutions at Ericsson. In this role he is responsible for end-to-end security management solutions including security automation and analytics. Mononen joined Ericsson in 1990 and for the past 15 years he has held leading positions in professional security services and in security technology development. He holds an M.Sc. in computer science and engineering from Chalmers University of Technology in Gothenburg, Sweden.

Patrik Teppo

◆ joined Ericsson in 1995 and is currently working as a security architect with the CTO Office, Architecture and Portfolio team. He is responsible for the security part of the Ericsson architecture and leads Ericsson's IoT security architecture work. He holds a B.Sc. in software engineering from Blekinge Institute of Technology, Sweden.

Timo Suihko

◆ joined Ericsson in 1992 and is currently working as a senior security specialist in the Ericsson Network Security, Security Technologies team, which belongs to Group Function Technology and Emerging Business. He holds an M.Sc. from Helsinki University of Technology.

References

1. **GSMA Remote SIM Provisioning Specifications, available at:** *https://www.gsma.com/rsp/*
2. **Official Journal of the European Union, May 2016, Regulation (EU) 2016/679, General Data Protection Regulation (GDPR), available at:** *http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&qid=1490179745294&from=en*

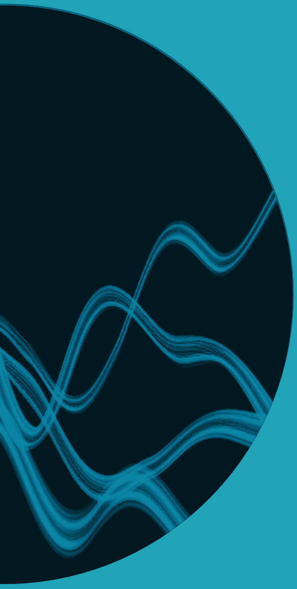
Further reading

》 **Ericsson white paper, February 2017, IoT Security – Protecting the Networked Society, available at:** *https://www.ericsson.com/en/publications/white-papers/iot-security-protecting-the-networked-society*

》 **Ericsson, Security Management, available at:** *https://www.ericsson.com/en/in-focus/security/security-management*

》 **Ericsson, Identity Management, available at:** *https://www.ericsson.com/en/in-focus/security/identity-management*

》 **ETSI GS NFV-SEC 013, V3.1.1, February 2017, Network Functions Virtualisation (NFV) Release 3; Security; Security Management and Monitoring specification, available at:** *http://www.etsi.org/deliver/etsi_gs/NFV-SEC/001_099/013/03.01.01_60/gs_NFV-SEC013v030101p.pdf*



ISSN 0014-0171
284 23-3305 | Uen

SE-164 83 Stockholm, Sweden
Phone: +46 10 719 0000