irdeto

Protect. Renew. Empower.

DATA SHEET

Irdeto Keys & Credentials for routers

Future-proof and take control over your CPE.
Secure your devices, brand and APIs.

The rapid evolution of Wi-Fi technology has made it a key feature for all broadband offerings to consumers and Small Medium Enterprises (SMEs). Routers are now fundamental to the Communication Service Provider (CSP) strategy.

They serve as the keystone for delivering advanced in-home services and ensuring a great customer experience. This is achieved through a combination of operator mobile apps and data-centric back-end services from a selected ecosystem of providers.

To leverage routers as powerful and flexible platforms for innovative value-added services, Internet Service Providers (ISPs) must retain full control over them and avoid being locked into proprietary stacks and security solutions.

Such lock-ins can slow down, fragment, or impede rapid innovation and the installation of new apps and features.

Additionally, smart Customer Premises Equipment (CPEs) are becoming increasingly attractive targets for cybercriminals, requiring a Security-by-design approach supported by industry experts.

Irdeto Keys & Credentials is a proven key lifecycle management service that enables ISPs to harden their routers and control the security assets of their CPEs, including those used to secure Application Programming Interface (API) communications, thereby avoiding supplier lock-in.

KEYS & CREDENTIALS FOR ROUTERS

Keys & Credentials (K&C) for Routers is a managed service that hardens the broadband CPE, including modems, gateways, routers and Wi-Fi extenders, by maintaining and renewing their platform security over their lifespan. K&C operates and automates all complex, technical workflows concerning the generation, distribution and renewal of cryptographic keys, certificates, hardware roots-of-trust and other assets. CPEs are deployed with advanced security features such as hardware-enabled code integrity and unclonable, unique Trusted Identities to secure all communications with the operator's core network or third party services – at a level of robustness that anticipates upcoming regulations.

The security of deployed CPE is actively maintained by means of the scalable, cloud-based Irdeto key management platform and the dedicated keying centers. The CSP retains control and ownership, therefore gaining independence from their suppliers, such as the Original Equipment Manufacturers (OEMs) and enabling the deployment of carrier-grade open-source platforms (such as RDK-B or prplOS) across its entire fleet.

KEY BENEFITS

Accelerate innovation

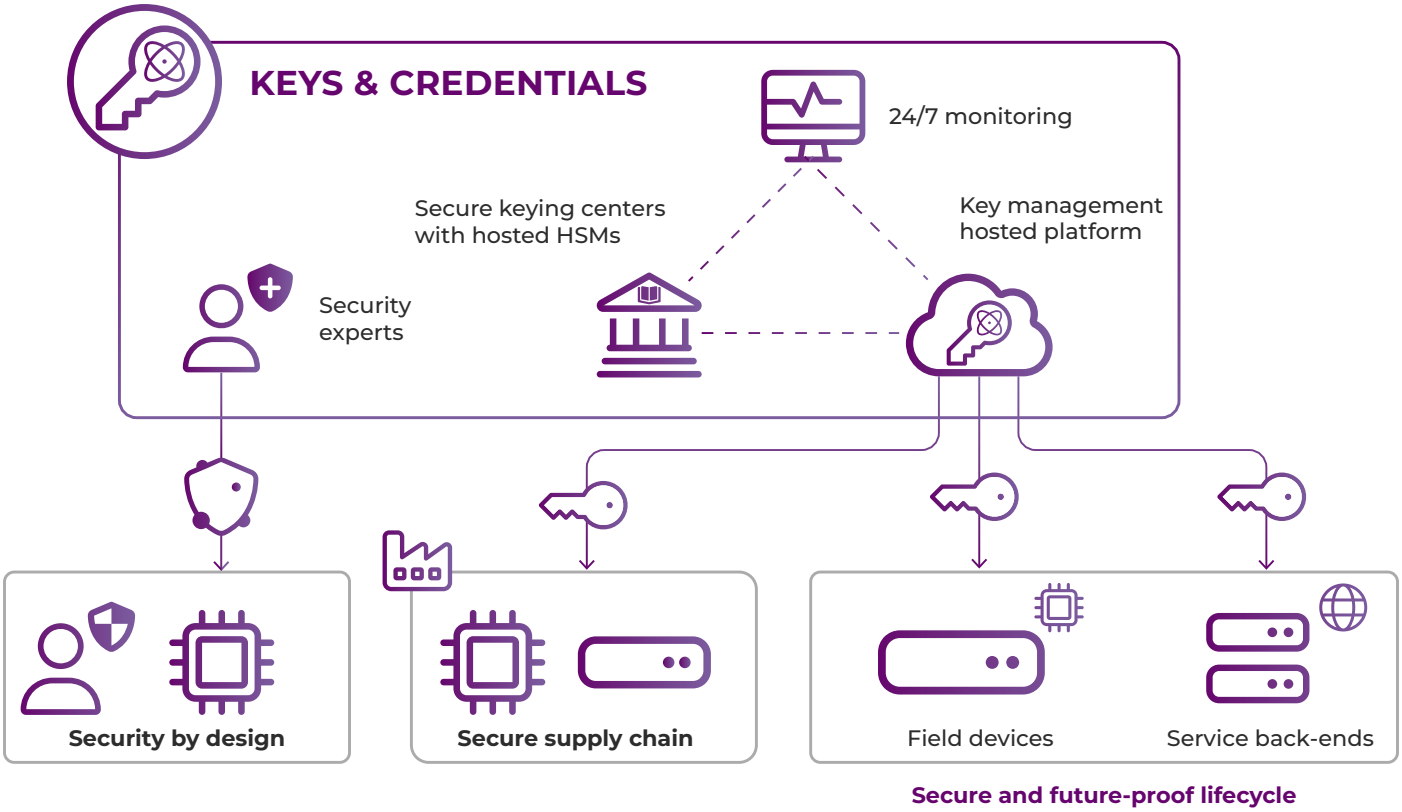
Thanks to CPE free from vendor lock-in. Quick delivery of innovative solutions across all OEMs and CPE models. Take full advantage of carrier-grade open system like RDK-B and prplOS.

Prevent costly attacks

By advanced malware that affects the operator brand, Irdeto protects the CPE and the core network with keys and certificates anchored into hardware.

Experts take care

Free up internal resources from in-house security workflows. Benefit from a wider pool of development resources, thanks to a CPE based on open APIs, standard technologies, with full control over security assets.



HOW IT WORKS

Security by design: For every new CPE project, Irdeto evaluates and integrates the cryptographic security foundations of the System on Chip (SoC) model, leveraging its expertise and partnerships. Due to the rising market demand in robustness, leading SoC vendors have introduced industry-proven hardware-based security features, such as Secure Boot, Trusted Execution Environments, One Time Programmable memory for credentials. However, even if supported by the SoC, the mechanisms must be explicitly activated for use during the design phase.

Secure the supply chain: The security foundation of a CPE must be embedded into the hardware during manufacturing. Irdeto generates, securely provisions, and tests operator's specific unique Trusted Identities (such as X.509 PKI certificates) into each CPE device at all production lines, by means of its keying centers and its cloud-based platform. The firmware release process is set up so that only the operator will be able to authorize new updates via signing keys hosted at the Irdeto keying centers.

Secure and future-proof lifecycle: Once deployed, the CPE device exclusively executes operator- authorized software or containers and securely communicates with the operator or with third-party services. Backends can enforce strong access controls and implement Zero Trust architectures by authorizing the CPE based on its unclonable Trusted Identity. Operators can use the Irdeto cloud-based platform to rotate, revoke or securely introduce new credentials therefore extending the CPE's lifespan, to meet the future business needs and new threats.

KEY FEATURES

Easy deployment and usage

- Rapid onboarding on the service cloud platform
- Web UIs for flexible operations and dashboards
- Managed tokens and on-site SW/HW appliances to secure all manufacturing and service processes
- Multiple environments to match the product lifecycle, from design to production

Easy authorization control

- Integrated user management
- Multi-factor authentication
- Role based access control allowing the definition of fine-grained authorization policies
- Profile-based logic to ensure that different projects are segregated with their own security policies

Easy automation

- APIs for in-field keying, renewal, revocation
- APIs for full automation of build pipelines
- Approval workflows for certificate issuance and firmware signing

Several types of cryptographic assets

- Private and Publicly trusted X.509 PKIs
- Unlimited number of CAs with arbitrary PKI hierarchies
- Code Signing keys
- DRM keys
- Symmetric keys (AES up to 256 bits) and passwords (e.g., JTAG credentials)
- RSA keys up to 4096 bits
- ECC keys up to NIST P-521
- Upcoming PQC algorithms
- PKCS#7 Code Signatures
- PKCS#1 v1.5, PSS, ECDSA and EdDSA

Integration with major silicon vendors

- Broadcom
- Qualcomm
- NXP
- Mediatek
- Realtek
- AmLogic

Service management, capacity, availability

- Up to 125,000 keys / hour
- Up to 99.95% availability rate
- 24/7/365 operations and support
- Security assets managed on behalf of the customer under Irdeto's SO 27001:2013 program
- WebTrust conformance
- Managed FIPS 140-2 Level 3 Hardware Security Modules, hosted at Irdeto facilities
- Business continuity and disaster recovery plans

Would you like to learn more about Irdeto Keys & Credentials for routers or explore how it can enhance your revenue?

Reach out to us today at www.irdeto.com!

Last modification: 19-06-2025 / 04:06 pm GMT+01:00