irdeto

Solution Overview

Irdeto Keys & Credentials for Routers

Protect ISP infrastructure and reputation with enhanced CPE resilience and recoverability

As consumers become increasingly dependent on connected devices in their homes, they are also becoming more aware of the security risks involved. They want an ISP they can trust to deal effectively with a new generation of cyber threats to their personal data and the physical security of their connected homes. But the routers and gateways supplied by operators to subscriber homes are already a top target for hackers and will become even more attractive as they evolve into application platforms. ISPs can face catastrophic costs and reputational harm if security breaches interrupt connectivity, expose subscriber data, or leave the ISP's own core infrastructure open to attack.

EXTRA TITLE FOR AT A GLANCE

Why should ISPs use Keys and Credentials for Routers?

1. To protect Customer Premises Equipment (CPE) from advanced malware and ensure these devices will only ever run the software and apps approved by the ISP, providing recoverability from router hijack attacks

2. To protect their core network (and the customer data it holds) from attacks using spoofed routers by adding an unclonable, Trusted Identities to all CPE

3. To maintain security while introducing innovative new consumer services via the home router or gateway, without the up-front and ongoing costs of establishing and operating their own security facilities

What is it?

A vendor-neutral suite of managed security services that covers the full security lifecycle of all broadband CPE including routers, gateways and Wi-Fi extenders. Irdeto takes on the role of Trust Authority for the operator, providing:

- Secure generation of code signing keys and related Trust Anchors for provisioning into CPE at the factory

- Management of code signing processes for all future software and firmware releases

- Secure generation of unique, unclonable Trusted Identities for provisioning into the CPE hardware at the factory

- Cloud-based distribution of new and updated security materials to CPE already in the field for the full lifespan of the device - including PKI certificates, master keys, API keys, SSH keys, wireless credentials, passwords etc.

- Revocation of access rights for any CPE known to have been compromised

- Vendor-neutral, independent services operated from high security facilities and high-availability cloud servers

- Expert security assessments to identify weaknesses in the CPE supply chain and recommend improvements to hardware and software configuration

EXTRA TITLE FOR AT A GLANCE

What are the business benefits?

- **Reduced risk** – adding a hardware-based security foundation to all CPE limits unauthorized access to the consumer home and the operator's own back end infrastructure, demonstrating resilience to attack and recoverability from breaches

- **Future proofing** – remote deployment of new and updated keys extends the lifespan of the CPE, enabling existing devices to adapt to changing business requirements

- **Flexible business model** – operators can select from a suite of services on a pay-as-you-grow model that reduces up-front costs and scales to meet evolving business needs

- **A true security partnership** – Irdeto's half-century of experience makes us an ideal Trust Authority to ensure the long-term protection of broadband CPE and assist in compliance with proposed IoT security regulations

- **Rapid deployment** – Irdeto's vendor neutrality and pre-existing relationships with many leading ODMs help to reduce project complexity when deploying new models of CPE and to ensure a consistent security posture across all models and vendors

Who is using it?

Irdeto's secure keying facilities have already generated and provisioned more than one billion individual security assets (keys and certificates) to in excess of 80 million individual CPE devices for Tier One operators in North America and Europe.

IRDETO KEYS & CREDENTIALS FOR ROUTERS

Our homes are more connected than ever before. Every day, consumers add new IoT devices, from webcams and games consoles to health monitoring devices and smart locks. The unsung heroes of this story are the routers, gateways and Wi-Fi extenders supplied by Internet Service Providers to support this growing connectivity. ISPs are increasingly looking to this customer premises equipment (CPE) to deliver new, revenue-generating services like whole home Wi-Fi management or intrusion detection.

But these devices are also a top target for hackers looking to gain access to the home, in part because they're implicitly trusted by both subscribers and their operators. ISPs treat CPE as an extension of their core network. Attackers see routers as an effective, scalable and largely hidden way to harvest user data, mislead users (diverting them to malicious websites), join botnets or target the ISP's core infrastructure. CPE is vulnerable to both external attack and internal threats from insecure IoT gadgets within the home. In the event of a full router hijack, the only ways to regain control may be replacing the hardware and/or requiring a technician visit. More than ever, operators must be vigilant over the security, resilience, and recoverability of their CPE.

Consumers need an ISP they can count on

Once, ISPs could satisfy consumers by focusing on broadband speed and a consistent connection at the right price. But as connected devices put the internet at the heart of our daily lives, security-conscious consumers are increasingly aware that weak networks can put at risk their sensitive and financial data, medical devices and even the physical security of their homes. They won't hesitate to switch suppliers if security breaches impact the reliability of their connection or jeopardize their personal data.

Insecure routers put ISPs at massive risk

An estimated 75% of all IoT attacks can be traced back to infected routers (w). Each of these compromised devices exists at the edge of an operator's trusted network. ISPs can face catastrophic civil damages and irreparable harm to their reputation when security incidents interrupt connectivity, expose subscriber data, or lead to a breach of their own infrastructure. Proposed IoT legislation in many markets could soon force operators to demonstrate effective mitigation strategies and the ability to recover quickly from such attacks.

Who's that knocking at the door?

Fundamentally, operators need to effectively manage access to the CPE. They must prevent bad actors from installing rogue software or apps on broadband devices to gain control over the home and its data (router hijacking) and have a robust approach to recovering from such attempts. At the same time, they must prevent CPE from being used to gain unauthorized access to their own infrastructure or the servers of their business partners (router spoofing). But security is not a core competency of the Original Design Manufacturers (ODMs) who supply most CPE. Too often, equipment is shipped with insecure software or hardware configurations, or with no consideration for how security will be maintained over the multi-year lifespan of the device. ISPs also lack the facilities, expertise or resources to maintain their own full-scale, multi-vendor CPE security program. They need an Independent Trust Authority to manage security on their behalf.

PROTECT SUBSCRIBERS AND YOUR NETWORK. PROTECT YOUR BOTTOM LINE AND BRAND

Irdeto Keys & Credentials for Routers is a unique solution, offering ISPs a proven suite of managed services that covers the full security lifecycle of all broadband CPE. It brings enhanced security, resilience, and recoverability to routers, gateways and Wi-fi extenders, as well as the flexibility to adapt them to future security needs. Unclonable Trusted Identities (in the form of keys and certificates) are provisioned in each device to support enhanced authentication processes and prevent spoofing. Meanwhile, managed code signing blocks the installation of malicious software on in-field CPE, ensuring ISPs can't be permanently locked out of their own hardware. Expert security assessments identify weaknesses in the CPE supply chain and ensure devices are shipped with the optimal configuration for ongoing security.

KEY BENEFITS: PEACE OF MIND

End-to-End security for all broadband CPE

Irdeto Keys & Credentials for routers gives operators confidence that the devices they ship will be secure from the factory floor to the last day of use in the subscriber home. Securely provisioned unique identities leveraging a hardware root of trust will underpin all future authentication. A wide range of additional keys and certificates can then be remotely provisioned to in-field CPE and updated or revoked to suit the operator's evolving security and business requirements, including emerging industry platform standards such as TR-369 (USP). Additionally, managed code signing provides peace of mind that the operator can always recover from attacks because malware and rogue firmware can't be installed to lock them out of the CPE. Delegating the management of these mechanisms to independent experts ensures a consistent security posture across all new CPE, no matter which hardware suppliers are chosen over time.

Protection for the broadband core network

CPE devices are treated as a trusted part of your network, but they're operating in an increasingly hostile environment. Embedding unclonable Trusted Identities into every router, gateway and Wi-Fi extender you deploy will give you confidence that your backend infrastructure is only communicating with genuine CPE. Keep the customer, billing and corporate data in your network safe from compromise to protect your brand and your reputation.

Your CPE security in expert hands, round the clock

When you delegate your CPE security to Irdeto as your Trust Authority, you benefit from our 50+ years of expertise in protecting digital assets, without the cost and hassle of establishing your own facilities or the ongoing investment in an in-house security team. We have strong relationships with all of the leading chipset manufacturers and have been providing key management services to Tier 1 operators in the US and Europe for many years. Our secure and high-availability keying facilities have already generated more than one billion individual security assets (keys and certificates) for factory or field provisioning to in excess of 80 million individual CPE devices. A 24/7 global support team ensures rapid response to any security challenges you may face.

It's our job to stay on top of all the latest industry guidance and legislation, advising operators on how to comply with new IoT regulations as they emerge. Our team can also provide independent assessment services for your entire CPE supply chain. Let us review the design, processes and configuration used by your current and future ODMs to identify any areas where security may be improved.

SOLUTION DESCRIPTION

The security architecture of all modern CPE platforms, no matter how complex, relies on a small number of critical secrets known as roots of trust (RoT). These may include Root Certificate Authorities (CA) in Public Key Infrastructures (PKI), master keys, code signing keys or non-renewable secrets permanently embedded in hardware. Because these RoTs are so fundamental to the security mechanisms, any loss or compromise of the secrets is highly damaging. They must be managed with high-grade security controls including dedicated physical facilities, offline networks, vetted personnel with specialized security expertise, thorough backup and business continuity plans. This type of activity goes far beyond the comfort zone of even the largest ISPs and ODMs.

Your independent trust authority

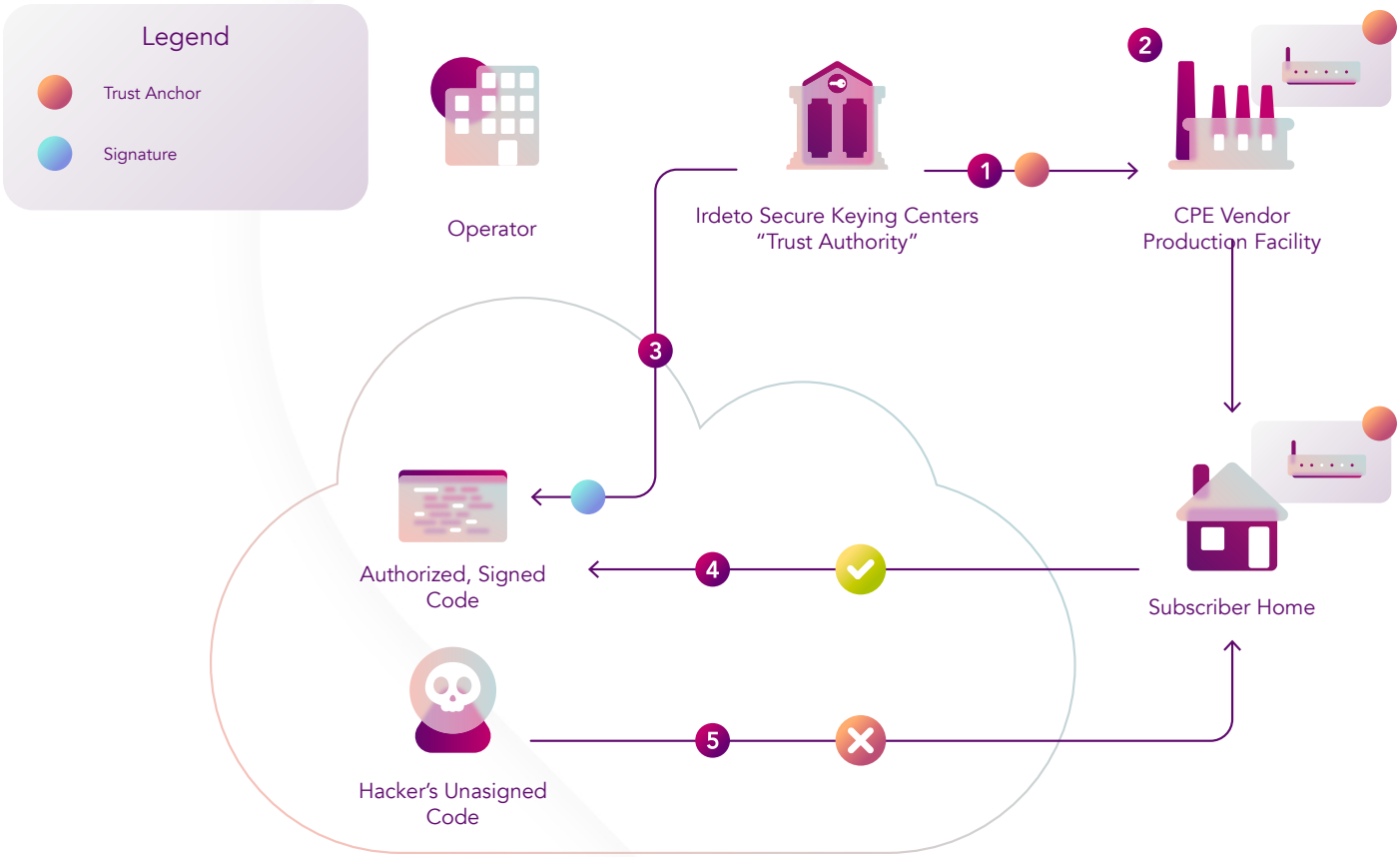
Irdeto already has all these elements in place and fully operational. No matter which combination of our router security services you select, Irdeto becomes your vendor-neutral, Independent Trust Authority, issuing keys, certificates and other credentials on your behalf. Our dedicated security centers are staffed by expert professionals running proven certification programs (including ISO 27001). All RoT secrets are securely managed with top-tier security controls and 24/7 support. Our pre-existing relationships and integrations with many leading ODMs can also reduce timescales for your new generation of CPE.

A range of services to future-proof your new generation of CPE

Managed code signing for malware resistance *(Figure 1)*

Secure (or verified) boot is one of the most important and cost-effective technologies available to make CPE resistant to router hijacking attacks that are malware-based or involve physical access to the device.

Each operator has their own unique code signing keys which must be stored securely. During the CPE manufacturing process, operator-specific credentials known as "Trust Anchors" are added to the secure boot feature in the CPE hardware. Once in the field, the device can immediately identify authorized software because it is signed using the operator's code signing key which is recognized by the Trust Anchor. Any attempt to install unsigned or falsely signed software, including malware or rogue firmware, will be rejected by the secure boot facility. Such protection helps ISPs to demonstrate true recoverability in the event of a router hack, because even attackers with physical access to the CPE cannot install their own firmware and lock the ISP out of the broadband home.



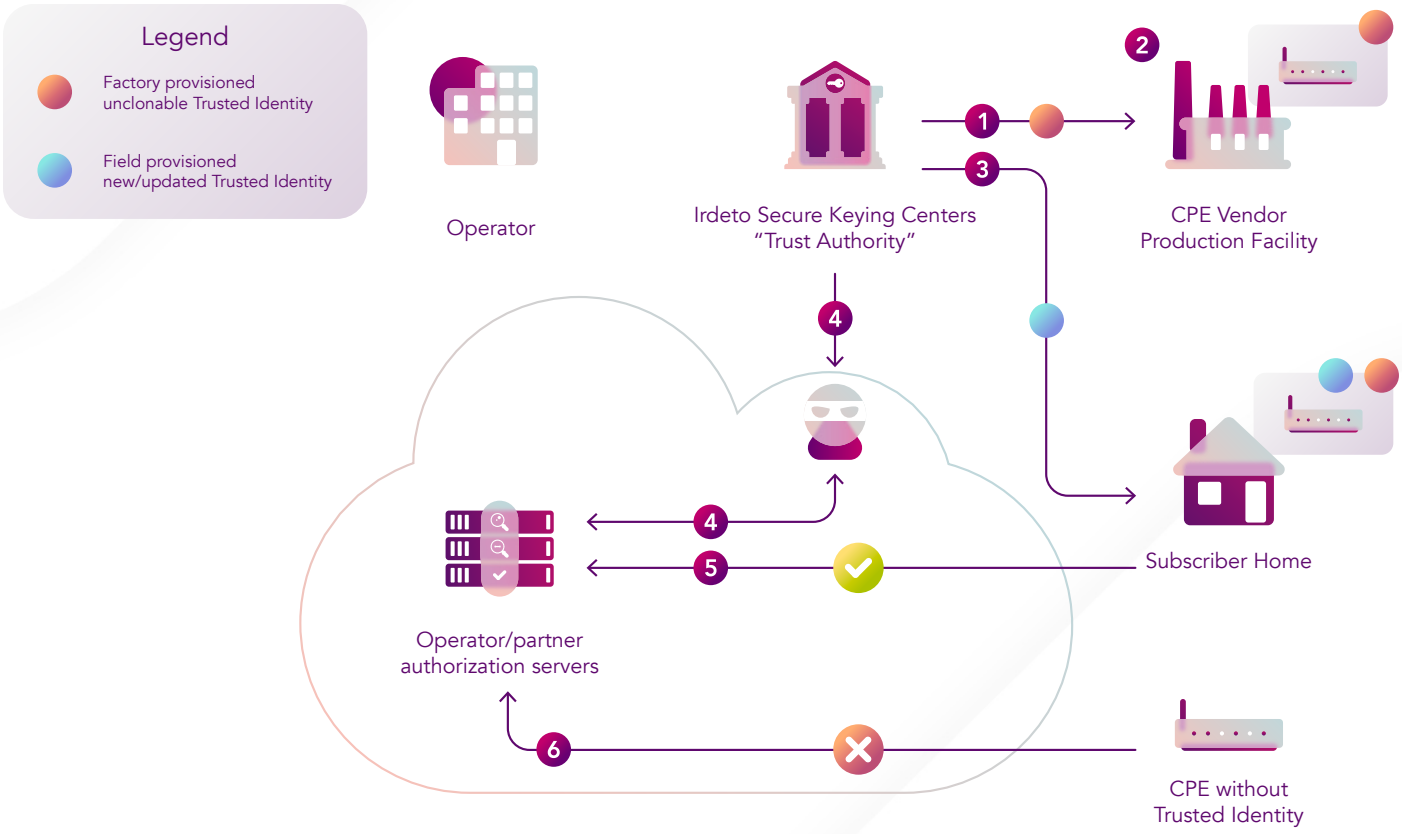
1. Irdeto's Secure Keying Center generates Code Signing Keys (CSKs) and Trust Anchors (TAs). TAs are securely delivered to CPE vendors. CSKs are stored securely in the Irdeto Keying Center.
2. A TA is added to the secure boot feature in each CPE hardware during manufacture.
3. Authorized developers submit their code to Irdeto for signature on behalf of the operator prior to distribution to the CPE.
4. The TA in each CPE identifies legitimate software authorized by the operator because it is signed using the correct CSK.
5. Any software that is not signed with the operator's CSK will be rejected by the CPE secure boot and will not run on the device.

Figure 1. Managed Code Signing

Though many CPE vendors already offer some degree of code signing, operators should consider whether they are storing the signing keys securely. Taking control of their own signing keys can give operators confidence that the keys will always be available to sign new software, even if their relationship with the CPE vendor breaks down, or the CPE vendor ceases trading.

With Irdeto's Managed Code Signing Service, operators can take control without taking on the responsibility and expense of managing them in-house. Code Signing Keys and related Trust Anchors for all new CPE are securely generated, backed up and protected inside online FIPS-certified Hardware Security Modules (HSM), fully under the physical control of Irdeto. Our experts deal directly with any developers authorized by the operator (including third parties) so they can easily define workflows with fine-grained policies and approval cycles to efficiently trace, sign, encrypt, and automate new firmware releases before roll-out.

Trusted Identities protect core networks from birth to death *(Figure 2)*
The transformation of CPE from simple connectivity device to an application platform means an increase in return communications from the CPE to backend servers in the operator's network and their partner ecosystem. Preventing attackers from cloning or spoofing CPE is an essential step towards protecting the operator's backend infrastructure from cyberattack. The smart way to achieve this goal is to establish a unique, unclonable Trusted Identity in each device during manufacturing. But each router or gateway is expected to operate for many years, and its security posture will inevitably change over that time. As the ISP's software stack evolves and new applications are deployed (both in the CPE and in the operator's backend), the Trusted Identity that was originally established in the factory may become invalid, insecure or unfit for purpose. With a hardware RoT still in place, it's possible to renew or revoke credentials as security and business requirements evolve.



1. Irdeto's Secure Keying Center generates and issues a Trusted Identity key for each CPE.
2. The key is added to the CPE hardware during manufacture creating a Root of Trust.
3. During the CPE lifetime, the operator can instruct Irdeto to issue new/updated Trusted Identity via Field Provisioning.
4. On behalf of the operator, Irdeto publishes a blacklist of compromised identities for real-time authorization queries.
5. API calls are accepted by the operator or their partner's servers if they contain a non-blacklisted Trusted Identity.
6. API calls are rejected if made without a Trusted Identity or with blacklisted identities.

Figure 2. Trusted Identities for New CPE

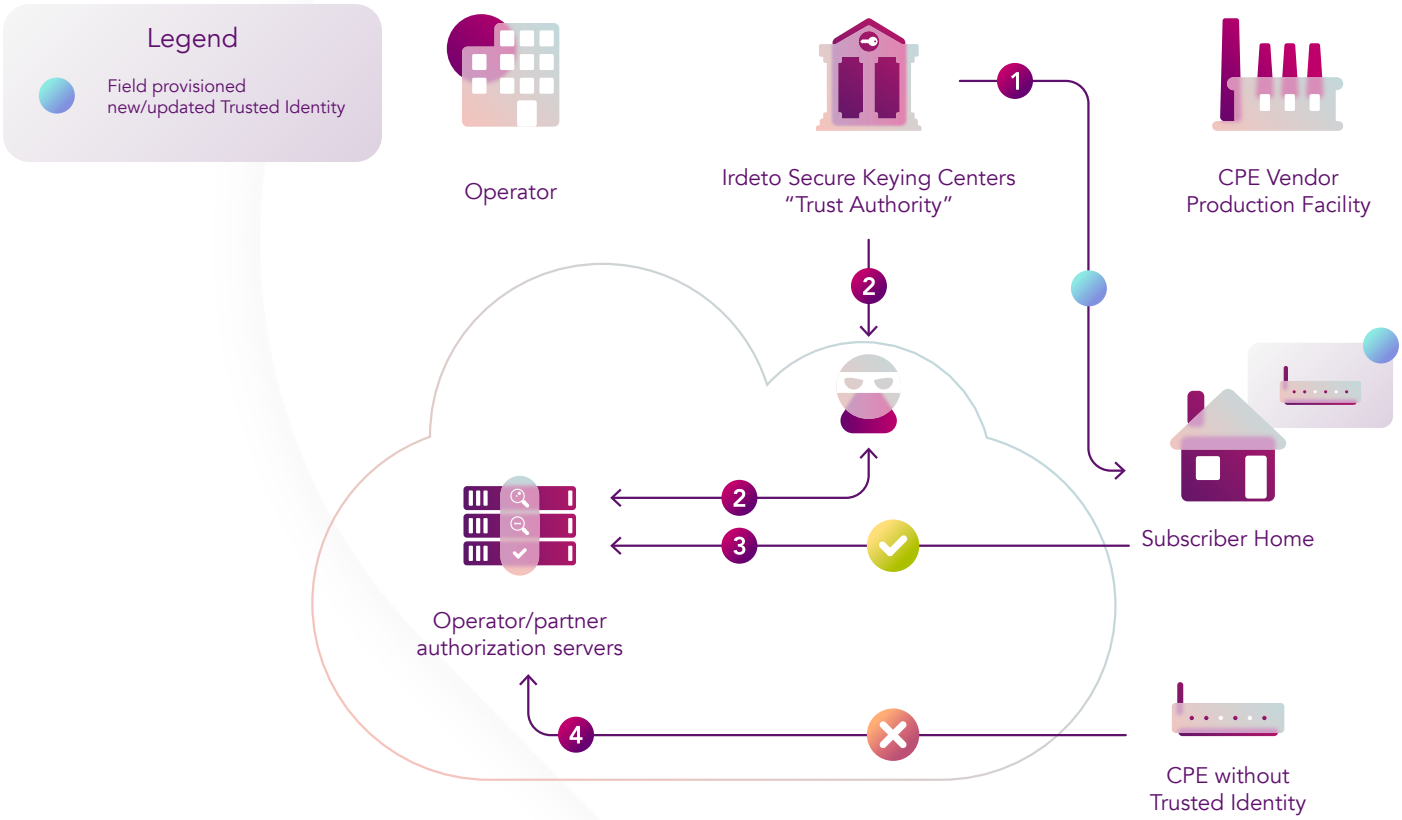
Factory Provisioning – Establish Trusted Identities
Irdeto's Trusted Identities service establishes unique credentials such as PKI Certificates into a hardware RoT in each CPE during hardware production. The router or gateway can then be authenticated with a high degree of certainty when it attempts to connect to the operator's network. The RoT and identity are individualized for the device and separate from any code signing RoT on the same CPE. Irdeto is also able to embed additional unique identities to further harden the device, such as JTAG debug passwords and SSH keys.

For every CPE model, Irdeto efficiently manages the integration process and the daily workflows with the relevant factories for the secure generation, distribution, and test of the Trusted Identities. These credentials are then provisioned into the CPE by the chip vendors, ODMs or contract manufacturers before shipment. Options exist for the deployment of on-prem black-boxes at chipset partners and OEM facilities to further enhance the security of the factory provisioning process.

Field Provisioning – Maintain the Trusted Identity
Irdeto's Trusted Identities service allows the operator to extend the CPE lifespan by securely and remotely installing new security assets, as well as renewing and revoking existing Trusted Identities connected to the RoT. For example, as the ISP's Certificate Authority, Irdeto can manage the full lifecycle of X.509 PKI certificates used by CPE to authenticate with operator or third-party services. Depending on the individual business need, we can also securely manage and distribute other assets on the operator's behalf including API keys, SSH keys, wireless credentials, and passwords. Where devices are known to have been compromised, or a shipment has been lost, Irdeto maintains and publishes a blacklist of CPE identities on behalf of the operator. These can be checked in real-time by any authentication mechanism that is operated by the ISP or its business partners. With Trusted Identity, it's also possible to take advantage of modern, advanced identity management practices which grant access to the core network based on short term certificates that are refreshed periodically across the entire population.

Field Provisioning is supported by a scalable and highly available cloud platform that generates Trusted Identities in real-time and securely distributes them to the CPE in compliance with the configuration defined by the operator. Each field provisioned Trusted Identity is protected end-to-end by the hardware root-of-trust established at the factory into each CPE, making it secure in transit and unclonable once installed.

Retrofit security to your existing CPE *(Figure 3)*
Although the gold-standard for CPE security involves factory provisioned Trusted Identities, we know operators also want to secure the legacy routers they've already got in the field. These older devices may not have a hardware RoT, but Irdeto can still field provision unique keys into each router to establish a Trusted Identity. This process uses the same scalable Remote Provisioning cloud platform described above, but also leverages Cloakware, our proprietary software protection technology. Cloakware obfuscates the remotely provisioned security credentials to frustrate hackers who might seek to extract or clone the device identity given the lack of RoT.



1. Irdeto's Secure Keying Center generates a Trusted Identity key for each CPE. The Trusted Identity key is remotely provisioning to each CPE. No Hardware Root of Trust is established, but the key is obfuscated with Cloakware Software Protection to protect it from compromise during transit and once on the CPE. During the CPE lifetime, the operator can instruct Irdeto to issue new/updated Trusted Identity via the same route.
2. On behalf of the operator, Irdeto publishes a blacklist of compromised identities for real-time authorization queries.
3. API calls are accepted by operator/partner servers if they contain non-blacklisted Trusted Identities.
4. API calls are rejected if made without a Trusted Identity or with blacklisted identities

Figure 3. Trusted Identities for legacy CPE already in the field

Expert reviews and security integrations

All Irdeto key management services can be complemented with specialized security consultancy to ensure operators get the very best use of the security hardware features available in their chosen CPE. The security architecture of the System-on-Chip (SoC) technology in today's CPE has improved significantly in recent years. It now includes fundamental technologies such as Secure Boot, One Time Programmable (OTP) memory and Trusted Execution Environments (TEEs). Our experts will review the design and integration employed by each ODM to ensure such features are being fully utilized.

Irdeto's security teams will also work directly with ODMs on behalf of the operator to ensure each CPE model is correctly configured and seamlessly integrated with Irdeto's key management services.

Lower your risk without exploding your costs

Until now, operators have had little choice over CPE security. They could ignore the risk completely, rely on whatever security management solution was offered by their various ODMs (with little or no oversight), or they could attempt to manage it in-house. But CPE security risk is no longer something ISPs can afford to ignore, and addressing it properly requires significant, long-term investment in secure facilities and expert staffing. Even the largest operators will find this an onerous burden on both capital and operational expenditure.

Irdeto's Keys & Credentials for Routers is a unique solution to these challenges. ISPs get rapid access to our highly available (up to 99.999%) cloud-based managed services and fully redundant secure physical keying facilities so they can start enhancing CPE security within weeks. The entire operation is staffed by security professionals with proven experience in delivering secure credentials to CPE, offering 24/7 global support and a true security partnership. The flexibility of our solution allows ISPs to enjoy a pay-as-you-grow model as they roll-out enhanced security to their CPE population, rather than facing heavy up-front investment.

SUMMARY

Broadband CPE is central to the modern connected home. With the advent of Mesh Wi-Fi, the number and range of CPE deployed is growing at a dramatic rate. CPE is also evolving into an application platform that delivers exciting new in-home services and generates revenue for operators. But these advances bring increased risk to both ISPs and their subscribers. CPE can be attacked from the open Internet and by unsecured IoT devices within the home. Hijacked or spoofed routers are a real risk to sensitive data, quality of service, the operator's core network and their brand.

Irdeto Keys & Credentials for Routers is a unique solution to these challenges, offering ISPs a way to build strong and dependable security foundation for the entire lifecycle of all broadband CPE. At the same time, the pay-as-you-grow business model and fully managed service enables operators to take control of their own CPE security credentials without the enormous responsibility and expense of managing them in-house.

Irdeto is the world leader in digital platform cybersecurity, empowering businesses to innovate for a secure, connected future. Building on over 50 years of expertise in security, Irdeto's services and solutions protect revenue, enable growth and fight cybercrime in video entertainment, video games, and connected industries including transport, health and infrastructure. With teams around the world, Irdeto's greatest asset is its people and diversity is celebrated through an inclusive workplace, where everyone has an equal opportunity to drive innovation and support Irdeto's success. Irdeto is the preferred security partner to empower a secure world where people can connect with confidence.

Last modification: 1-11-2021 / 03:52 pm GMT+01:00