escrypt
SECURITY. TRUST. SUCCESS.

Production Key Server

Secure Key Injection in Mass Production

Continuous supply of cryptographic keys and certificates

Modern embedded devices are becoming increasingly complex, feature-rich, and connected to other devices and the internet. However, this also makes them more vulnerable. To thwart the inherent security risks, embedded devices rely on a growing number of protective measures, the core of which is formed by modern cryptography based on keys and certificates. ESCRYPT has packaged many such measures in its Key Management Solution (KMS), which covers the complete security life cycle.

Device security has to start in production. Devices need to be provided with certificates as trust anchors, device-specific keys for authentication, and key material to protect interfaces. Only then is it possible to implement further use cases, e.g. provide secure access to the devices based on relevant certificates.

The optimal security solution has to combine three central aspects: first of all, the cryptographic material required during production must be hosted within the production environment. This ensures availability and low latency. Second, the solution must protect this cryptographic material with a hardware security module.

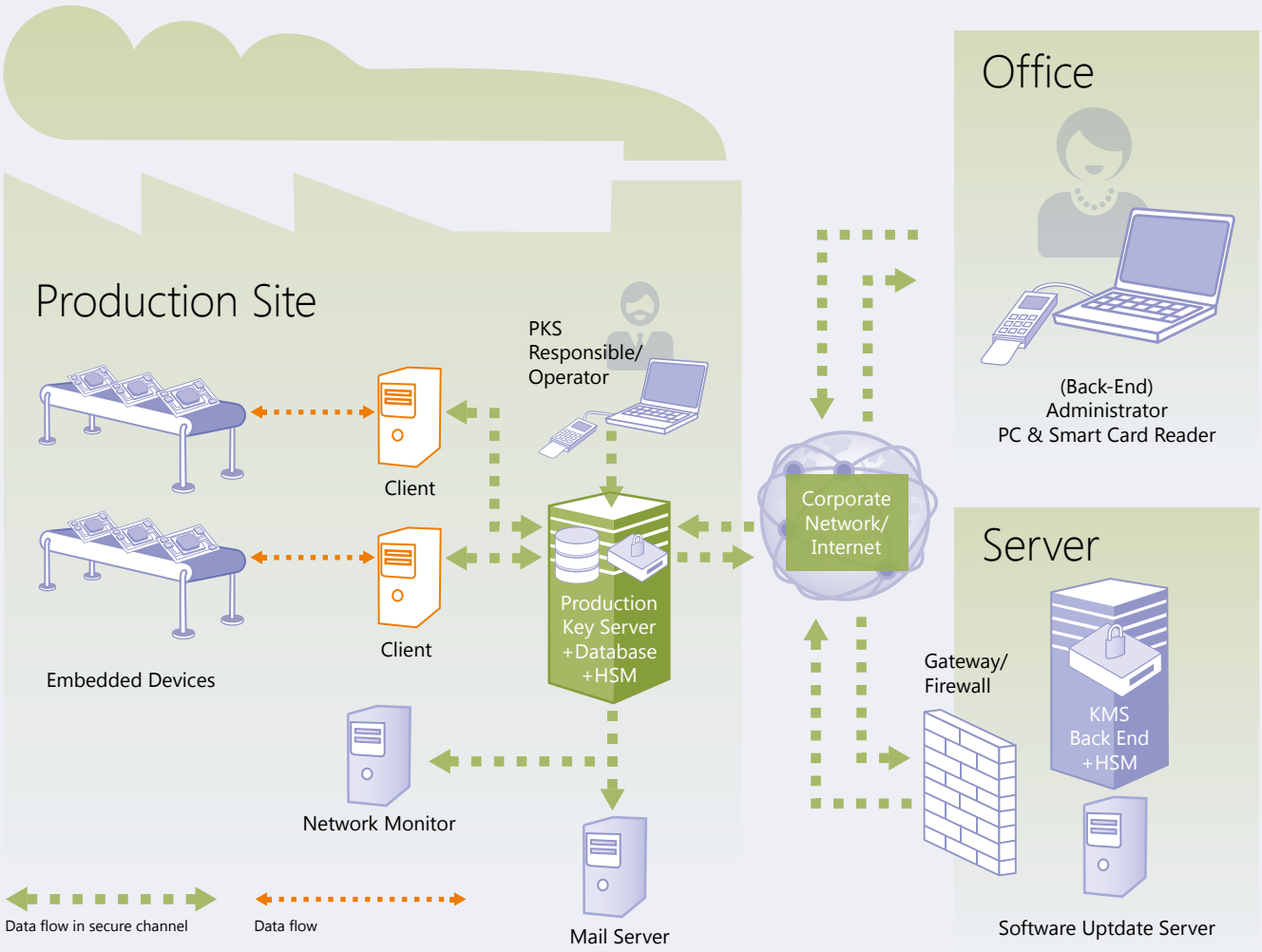
At the same time, it has to limit that material and usage of it in order to provide the necessary protection against attacks. And finally, the local solution server must periodically connect to a key management back-end; this allows keys to be provided to the production environment and also enables central monitoring, logging, remote administration, and reconfiguration.

ESCRYPT's Production Key Server (PKS) combines all these features in one product and thus provides production sites with a secure solution that is highly reliable, available, and maintainable. It makes certain that cryptographic material is injected during device production and enables corresponding end-of-line security testing and, later, product-return analysis. The PKS is part of ESCRYPT's Key Management Solution with a central back-end infrastructure for managing keys as well as access rights to those keys, including the corresponding monitoring. One of the PKS's main features is that it works without a permanent connection to any back-end infrastructure, but still guarantees a secure continuous supply of cryptographic keys and certificates.

ESCRYPT 2018/05

escrypt
SECURITY. TRUST. SUCCESS.

Production Key Server



Use cases

- Key injection (SHE keys, symmetric/asymmetric keys) for secure boot
- Installing trust anchors for SW update
- Issuing device certificates for M2M communication
- Local buffer for / generation of various keys and pass-words from OEMs and other 3rd parties (SHE keys, DTCP, debug passwords) for DRM
- Local authentication server for secure access and unlock-ing for end-of-line testing

Our Services at a Glance

- Solution consulting
- Implementation of custom functions
- Setup support
- Continuous updates and maintenance

Your Benefits

- Continuous high performance and secure supply of cryptographic material
- High availability due to independence of permanent back-end connection
- Specially designed to meet factory requirements
- High reliability and maintain-ability
- Centrally administered via ESCRYPT's KMS back-end

Any Questions?

Please contact us any time at
info@escrypt.com
or via phone:
+49 234 43870-200