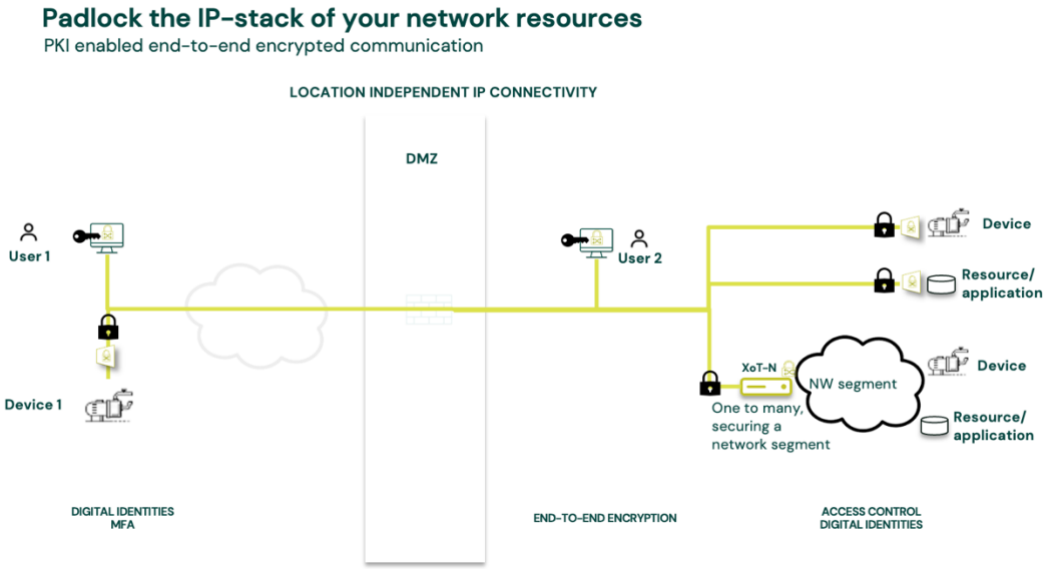
XoT technology™ Explained

What it is:

We develop and deliver an identity-based access control solution for connected devices in IT/OT and IOT (IIOT). The solution complements existing tools and techniques and will allow any type of equipment to be operated on any type of network, with full security. XoT technology™ brings undeniable digital identities and full end-to-end encryption out to any device using the IP protocol and a standard network interface, wired or wireless. The solution is based on three components; a client software for any type of end-user equipment (computers, tablets, phones etc), a security proxy HW (XoT-S1, placed close to the unprotected device) and a management system (XMS) that establishes connection rights based on policies and rules. Virtual products are aimed primarily at remote access capabilities, securing network segments or cloud applications rather than dedicated devices, and complements the solution to meet a wide variety of customer demands and needs.

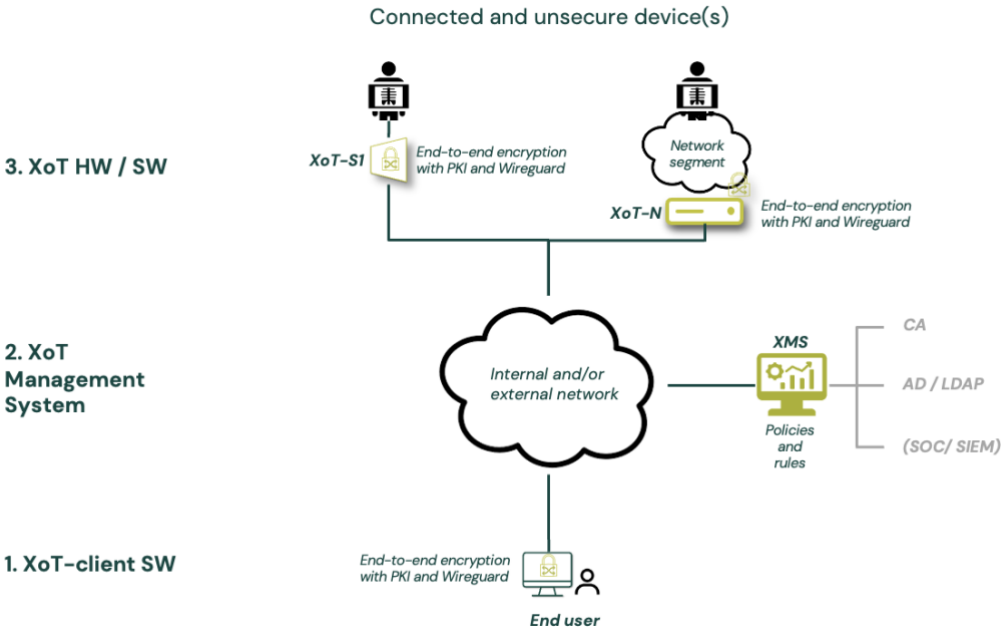
In essence, we have developed a unique cybersecurity solution that secures each connected device individually instead of securing the network. Our innovation complements existing tools and techniques and will allow any type of equipment to be operated on any type of network, with full security. A combination of current security measurements keeping the network safe with our solution for ensuring that only trusted users can access trusted devices will establish a solid security. XoT technology™ brings undeniable digital identities and full end-to-end encryption out to any device using the IP protocol and a standard network interface, wired or wireless.



XoT technology™ is a "drop-in" technology that can be applied to any type of underlying network, even those comprised by equipment from a broad range of

vendors and using a variety of protocols and techniques. XoT technology™ control the access on IP traffic level for any type of device using that protocol and some version of a standard connection port, fixed or wireless. The end user will not notice the addition of XoT technology™ in their daily IT or OT tasks and work efforts.

How it works:.



XoT technology™ is a fully agnostic security solution, easy to implement and manage. For any type of device and network.

When a connection is to be made from the end user to the now protected device, the client SW (nr 1 in the picture above), installed on the end-user device of choice, will use a unique and undeniable personal digital identity/certificate for the end-user in question. This certificate can be stored either as a soft certificate on the actual end-user device or, in order to create a higher level of security, on a physical token to create true multi factor authentication where the certificate cannot be distorted or copied. The important part here is that the solution is agnostic in relation to how the end user is identified, it is fully decided and controlled by the customer.

The XoT HW security proxy (nr 3 in the picture above), placed in front of the device that shall be protected, will investigate the credentials presented and communicate with the management system (nr 2 in the picture above) for approval of access. This access is given on user group level, i.e., for a dedicated user, belonging to a group of

users who share the same rights/permissions. Access rights are given based on two or three components: what TYPE of device it is, WHERE the device is located and WHEN the access attempt is taking place.

XoT technology™ is easily installed by the partner, or the customer by themselves as follows:

1. The management system (XMS) is installed either on a Kubernetes platform, hosted at the discretion of the customer, or as a virtual machine using Docker. Docker is a set of platforms as a service product that use OS-level virtualization to deliver software in packages called containers. This installation is a matter of a few hours and follows all current methods and best-practice processes.
2. Once the XMS is installed, a connection is established to a source of users and user groups, normally done through an Active Directory (AD) or any similar system using the LDAP protocol. This could be a more refined system such as IAM, IGM or PAM. The XMS only wants/needs to receive user data regularly, for instance every 15 minutes, to always be up to date. Any change in the AD or similar system will be easily propagated to the XMS for further accurate usage.
3. The second connection is made to the customers Certificate Authority system (CA), and XoT technology™ supports any such system that can operate using the standardised REST-API. The CA system is responsible for creating and revoking certificates throughout the use of the solution. Here again XoT technology™ is fully agnostic as it supports any type of CA system or certificate infrastructure, with the aim to enable a smooth implementation and a swift increase in security without having to restructure the entire IT network in preparation.
4. The customer now has an operational system in place, and all this within a single day. The next step is to set up the system regarding WHERE all devices are located and this is done through a tree-branch structure, defined by each customer according to their specific needs and requirements. A normal way could be Country / City / Street Address / Building / Room, but the customer can decide freely how this is done to meet their demands and maturity. This can also be easily changed over time to adhere to changes from an evolving organisation.
5. The last thing to be set up is TYPE of devices, i.e., how does the customer want to divide all their connected devices. Again, this is a solution with full freedom to support each customer's needs, and a simple example could be to at the top level divide the devices between "Network equipment", "Office equipment", "Production equipment" and "Security equipment". Below each of these groups the customer can divide further and for instance have a sub-group called "X-ray machines Chicago south" or "Printers Oslo".

Once the system is installed it is time to deploy the security onto all connected devices and this can be done by almost any employee. What is required is physical access to the devices, a smartphone and trust by the organisation. The individual to

deploy will take a number of XoT HW units with him/her and start deploying in a swift and simple fashion. First, identify which machine you want to secure. Enter that room and disconnect the device from the network and place that network cable into the XoT HW unit instead. Take a new and short cable (1-1,5m) and connect from the XoT HW unit to the device. All traffic will now flow through the XoT HW unit. Next step is to connect the XoT HW unit to power and boot it up. During the boot process the XoT will create its own private certificate (digital identity) and store it on a secure chip under a layer of epoxy so that it cannot be tampered, altered, or extracted by an unauthorised person, for instance a hacker, whether they are on the internal network or trying to access this device remotely.

The XoT HW unit will when booting up also display a unique QR code on the onboard screen, a code that will verify that it is a true XoT unit, and this identity is based on factory implemented root certificates. The deployment resource takes a smart-phone and reads the QR code that will connect them to the XMS and through a simple structure then choses WHERE they are and what TYPE of device they are securing. A photo, taken with the camera in the smartphone adds the last information and when pressing "DEPLOY" all is now done. It's a process that takes less than 3 minutes and requires no configuration of the protected device and it can be performed by anyone with a reasonable level of trust in the organisation. This way of securing devices is called "zero touch deployment" and together with the ability to secure any type of device truly shows how agnostic and easy to use XoT technology™ is.

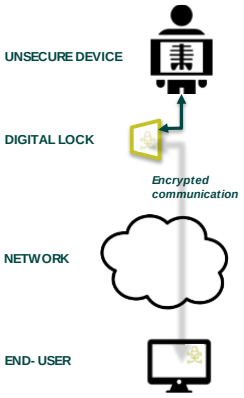
What remains now is setting accurate access policies to allow the right users access to each device and keeping everyone else out. Each policy takes about 20-30 seconds to create and includes the following steps:

1. Choose user group(s) for the policy, i.e., who shall be given rights to access the device in question.
2. Choose what TYPE of device this policy shall concern. This can be on highest level, e.g., "Production equipment" or on a lower level, e.g., "Industrial robots Factory 4 Alabama".
3. Choose WHERE this access will be granted, and here again this could be done on any level from Country down to a specific room in a known building.
4. Press "APPLY" and the policy will be valid in less than 30 seconds.

If a specific user/employee leaves the company, they will simply be taken out of the underlying user group in the end-user system, such as Active Directory, and thereby lose all access rights within XoT technology™. If an employee change position, they will quickly and simply be moved to a new user group and inherit all rights as per this user group. The essence of this approach is a key one when it comes to true cybersecurity.

Never give access rights to an individual, always give rights to user groups. But, and this is important, always verify the specific identity for each end user.

Why XoT technology™:



- A digital lock, preventing unauthorised access
- Secures critical devices within minutes
- Requires no configuration of clients or protected devices
- Brings undeniable digital identities to legacy systems
- Secures the traffic between devices and users
- High level security for any type of device

Key benefits with XoT technology™

XoT technology™ uses two layers of encryption, PKI and X.509 for certificate exchange, challenge response and system verification. PKI has several benefits with its asymmetrical structure, one of them making it difficult to hack, the other one that is a standard since late 70's, albeit constantly improved, with for instance elliptic curves being added to improve security and performance.

All payload transmission is done using session-based encryption keys and the Wireguard protocol, a protocol rapidly gaining traction in the industry. This way the current XoT HW unit can deliver up to 150 Mbps full encrypted traffic, 24/7.

With a set of HW products, virtual appliances, and several ways to identify end users, all controlled by a simple and secure management system (XMS) we will create a solid eco system for connected devices.

Physical products will include three main units; the current XoT-S1, suitable for one-to-one implementations close to the device, delivering up to 150 Mbps full wiregurard encryption. A soon to be developed XoT-S1/I, a IP-65 enclosed XoT-S1 with the same capacity but with ability to be implemented in adverse environment and handling heat, cold, moist and dust. The final physical product in the current plan is the XoT-R12, a 19 inch rack-based security unit, putting 12 security proxies (all of them hardware

separated) into one unit. A port nr 13 controls the whole rack and allows an air-gapped OT network to suddenly be managed remotely. In this rack unit the capacity will increase to 1Gbps full Wireguard encryption per channel, i.e., in total 12Gbps throughput at full speed.

Complementing this set of HW products are a few virtual ones. The XoT-N can secure a whole network segment, OR handle high-capacity loads well over 1Gbps. The XoT-C can secure cloud applications and systems and the XRA (XoT Remote Access) bridges between secure and unsecure networks, such as IT and OT or to/from Internet based users or equipment.

Our eco-system for solid access control: