intertrust® | DigiKoo PART OF e·on

Solution Brief

Platform

Explicit Private Networking (XPN): An indispensable tool for ensuring trusted data in distributed energy

The electric grid was originally designed as a centralized system where energy flowed in a single direction–from generation, transmission, distribution to consumption. Very little information flow was needed.

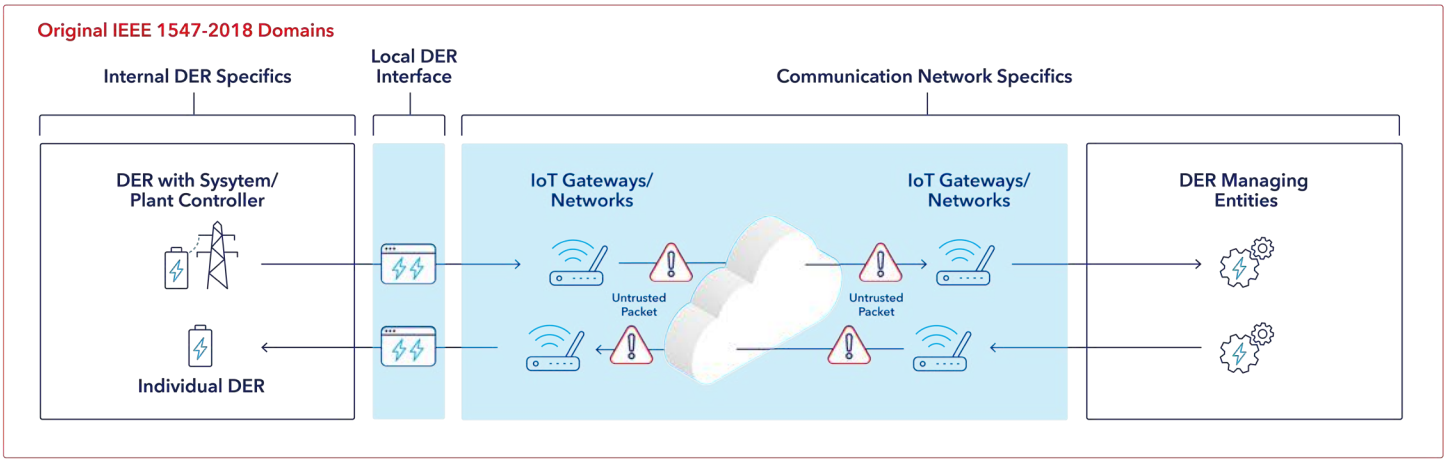
The evolving nature of the electric grid

The electric grid was originally designed as a centralized system where energy flowed in a single direction – from generation, transmission, distribution to consumption. Very little information flow was needed. In fact, the grid is becoming increasingly decentralized and automated. Energy is now being pushed to the edge, involving a wide array of new device types including EV chargers, inverters, hydrogen electrolyzers along with a myriad of consumer and industrial IoT devices. Decision making for distribution and load management is now done locally and in real time. The data flows to support this new grid, sometimes referred to as the Smart Grid, is also decentralized.

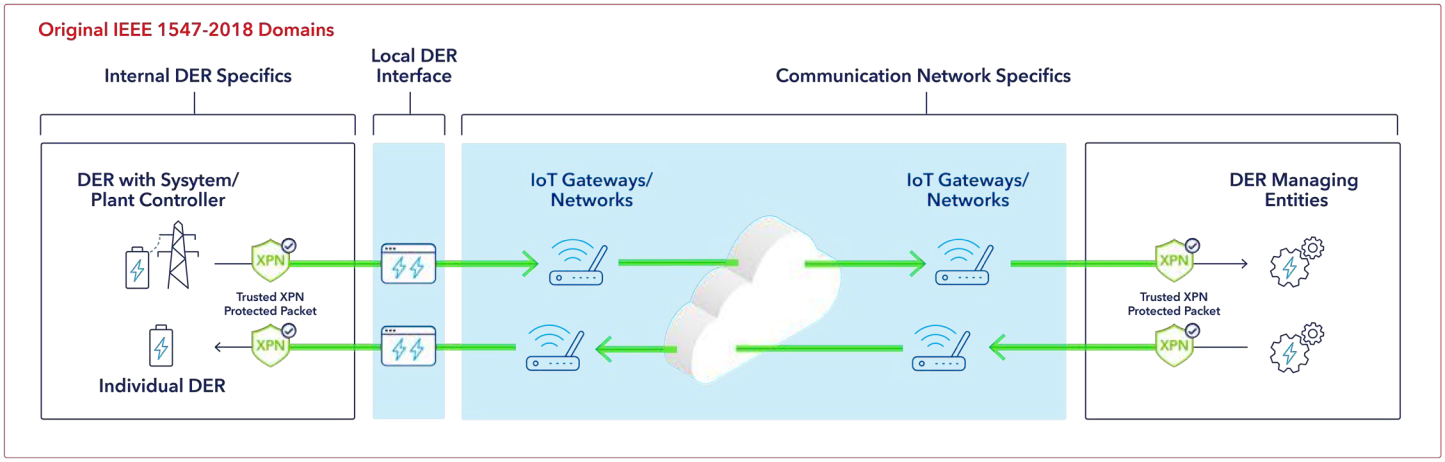
Today's Smart Grid consists of many distributed devices communicating over many different networks with a wide variety of security models and intersection points. This complexity makes distributed trust difficult.

The nature of this system is that many stakeholders in Smart Grid applications require distributed trust and device authorizations at the edge. Since such applications are data driven, it is essential that the data itself remain trusted as it traverses across untrusted gateways, Field Area and Core Networks. The intersection between Operational Technology (OT) and Information Technology (IT) systems is a critical exposure point as are the IoT gateways in Field Area Networks (FANs). Since so many networks have inadequate security and cannot be trusted, Zero Trust has risen as the preferred network model. The solution is to leverage trust in endpoints, both at the edge and in the cloud. This can be done with Explicit Private Networking (XPN. Similar to IPSec/ Virtual Private Network (VPN technologies in its aspirations, XPN actually protects data through untrusted gateways and networks because the end points are trusted. This trust is leveraged to protect the data as it travels over networks and reaches the cloud. This complexity is illustrated below.

DER ecosystems before XPN



DER ecosystems after XPN



XPN scales particularly well in complex distributed energy resources (DER) because distributed trust is required. Prior to XPN, enabling distributed trust in DER ecosystems has been difficult because all DER devices, their networks, and their managing entities exist in different Public Key Infrastructure (PKI) key spaces. This situation increases the complexities involved with security coordination between the different partners.

With XPN, trust is no longer dependent on technologies that only protect data in the "pipe" of the original network segment. It is now extended to the actual generation of the data from a sensor through to the ultimate consumption of that data. Truly end to end distributed trust is essential for Smart Grid applications and this is exactly what XPN offers.

DigiKoo[1], a subsidiary of the European energy giant E.ON, is an innovative company focused on a foresight platform and data-driven Smart Grid applications. "Electrical energy customers naturally expect reliable, trouble-free delivery of electricity," note Martin Moeller and Benjamin Jambor, from DigiKoo. "XPN will help us ensure that the DERs and data that drive the new clean energy grid are not a weak spot in the reliable flow of electricity." As automation, computing and communications increase at the edge, we will witness an increase in the use of actuators in machines to do work based on the data they receive. While malicious data injected by bad actors will pose a serious threat for sensors, it is even more threatening for these actuators because malicious data can make machines do dangerous things.

How it works

Each end point will have an XPN client installed. The XPN client will be protected to ensure that sensitive processing will be done in a Trusted Execution Environment (TEE) on the end point and sensitive key material is stored only in secure storage. Device software is expected to be digitally signed so only known good software will be running on the end point verified by the Trusted Boot process at startup.

The XPN client will rely on these secure foundations of TEE, Trusted Storage and Boot to ensure resilient protection of data. These foundations are enabled through a combination of PKI toolsets and integration with the hardware security of the chips.

When analog inputs are sensed by the sensor, it will process the input through an Analog/Digital converter (A/D). As soon as the digital data is generated, the XPN client will access that buffer and sign it with XPN keys for a particular trusted key space. Signing ensures both the authenticity of the data originating from the specific end point and its integrity is assured by the SHA-3 hash. Optionally, if the information is sensitive, it can also be kept secret by encrypting the data.

XPN packages have routing data for the consuming server. The consuming server is, itself, an XPN end point and a feature of Intertrust Platform.[2] The server will perform a digital signature verification to validate the authenticity and data integrity of every data packet. If encryption was applied, it will decrypt the data into plain text. Further collaboration and sharing will be managed using the features of Intertrust Platform.

Beyond electricity

The electrical energy industry is not the only one that needs a solution for overcoming risks associated with insecure field area networks. All utilities have embraced the benefits of digital transformation. Increasingly water and gas utilities are connecting their meters to field area networks and using the data to transform the delivery of water and gas to be much more efficient. XPN is application and network agnostic, it is optimized for the delivery of trusted data regardless of the target application or connectivity used.

Conclusion

Focusing on data authenticity and data integrity provides persistent protection of data through zero trust networks and across untrusted gateways and routers. XPN ensures data from sensors can be trusted, and this trust can be maintained in its journey to when it is sent to actuators. It is the missing element in securing machines in an industrial context and can be extended further to P2P communications, and value exchanges. With rich permissions enforced at the generation and consumption of data, XPN introduces significant distributed trust in modern energy systems and supports any number of use cases in the industry.

1 For more information on DigiKoo, please visit https://digikoo.de/en/

2 For more information on Intertrust Platform, please visit https://www.intertrust.com/platform/

intertrust®

Building trust for the connected world.

Learn more at: intertrust.com/platform
Contact us at: +1 408 616 1600 | dataplatform@intertrust.com

Intertrust Technologies Corporation
400 N McCarthy Blvd, Suite 220, Milpitas, CA 95035