UBIQUITY

Security Architecture White Paper

Last update: 2023/05/26

Summary

Abstract 1

Audience 1

Design Consideration 1

Component Architecture 1

Network and Protocol Design 2

- Access Server and Web API 2
- Relay Servers 3

Transport Security 3

- Access Server Connection 3
- Relay Server Connection 4
- Web API Connection 4

Remote access tools security 4

- VPN 4
- File Transfer 5

Authentication 5

- Authentication of Users to Servers 5
  - Two-Factor Authentication (2FA) 5
- Authentication of Runtimes to Servers 6
- Authentication of Access Servers to Frontends and Runtime 6

Operation Audit 6

Authorization 7

Cyber-attacks Countermeasures 7

- Brute force detection 7
- Password management 7
- Code Signing 7
- Man-in-the-middle 8

Datacenter 8

- Security Standards 8
- Backup 8

Software Updates 8

Data Breach Policy 8

Best Practices 9

Abstract

This paper provides a description of the network architecture and security design of ASEM’s UBIQUITY solution.

Audience

This document is aimed to network administrators, security auditors and decision makers to have a complete description of the security management and design to evaluate if UBIQUITY is compliant to their security standards and their use case scenarios.

Design Consideration

UBIQUITY’s core task is to securely connect a client to remote devices through the Internet (considered an insecure network). Thus, security is paramount on all design and implementation decisions, more than any other usability aspects.

Component Architecture

UBIQUITY Runtime	The software service that runs on remote devices to allow remote access to the device itself from Frontend clients. The Runtime is available for open systems such as Windows boxes and for closed systems, such as ASEM’s industrial routers. The same security considerations apply.
Access Servers	Access Servers are a distributed redundant set of servers that enables devices connection and provides a rendezvous for clients to connect to devices.
UBIQUITY Domain	It is a logical container that stores all resources of a customer account: users, groups, devices and their configurations, folders, authorization rules and logs.
Control Center	The interactive rich-client allows users to login into their UBIQUITY domain and connect to remote devices that run UBIQUITY Runtime. Administrative users can also use Control Center to manage the security rules and the configuration of devices. Subsequently, it will also be generically referenced as a Frontend client.
Control Center Web	The interactive web client allows users to login into their UBIQUITY domain and connect to remote devices that run UBIQUITY Runtime. Administrative users can also use Control Center Web to manage the security rules and the configuration of devices. Advanced functions like VPN are achieved by using applets (Tools) that can be started directly from the web browser. Subsequently, it will also be generically referenced as a Frontend client.

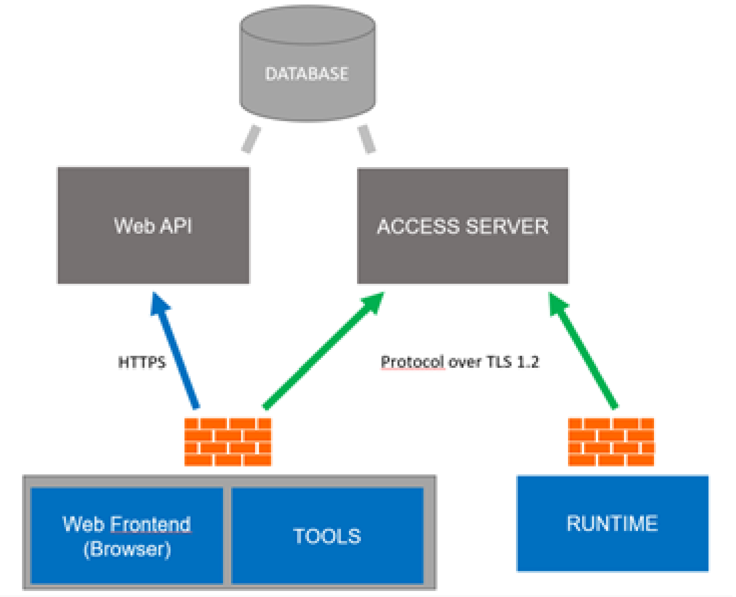
Relay Servers	They are servers located on all continents and they act as a public relay endpoint between Control Center and Runtime. They are not directly exposed and reachable through the Internet.
UBIQUITY Web API	It exposes the API needed by the Control Center / Control Center Web, and the Tools Applets to work and other auxiliary facilities such as software updates and requiring password reset links.

Network and Protocol Design

To better understand the security architecture, it is important to have a brief understanding of the described components and how they work together.

The architecture can be divided in two parts, one supporting client connection and authentication and one supporting Frontend to Runtime connection.

Access Server and Web API



Simplified network schema

The authentication to the UBIQUITY Domain is done by the Web API for the Control Center Web and Tools and by the Access Server for the Control Center and the Runtime. The UBIQUITY Domain information is stored in a database that is behind the Web API and Access Server.

All clients are assumed to be configured behind a firewall that only allows outgoing connections. The connection from clients to the Access Server uses TLS 1.2 with certificate authentication.

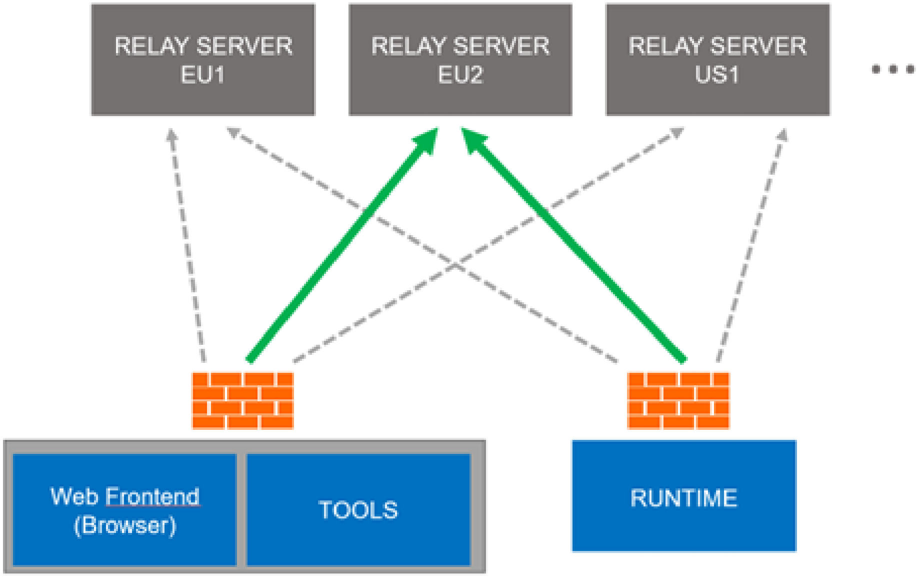
Clients can use the default TCP 443 outgoing port or can be configured to use port 80 or 5935 (TLS is still used of course), depending on what is best to comply with local IT policies. Clients automatically test available outgoing ports, but they can be configured for a fixed port.

Access Servers are redundant and fault tolerant. They are reachable by a couple of exposed endpoints and clients should be able to reach both for best service availability.

Web API is a ReST API that offers authentication/authorization and administration functions to frontends, such as administering folders, devices, users, groups, and so on or getting software updates download URLs. HTTPS is used for connecting to such service.

Relay Servers

When there is a remote access session between a Control Center Web, a Tools Applet or a Control Center and a Runtime, a Relay Server is used for data forwarding. Relay Servers allow both Frontends and Runtime to stay safe behind their firewalls as no incoming ports on their side must be open.



Frontend and Runtime automatically choose the relay server to use from a pool of available list of servers list, provided dynamically by the Access Server.

In order to select a best Relay Server for a certain remote access session, both Frontend and Runtime perform a connection test to all relay servers and measure their respective network performances.
Both Frontend and Runtime results are then combined in order to select the best relay.
This automatic behavior can be disabled, and clients can be configured to use a fixed relay server.

Transport Security

Access Server Connection

TLS 1.2 connections are used for the connection between clients and the Access Server. The following minimum cipher suites are used by the clients:

Cipher version	TLS v.1.2
Key exchange	ECDH (Elliptic-curve Diffie–Hellman)
Authentication	RSA
Encoding	AES-256
Mac (Message Authentication Code)	SHA-384

This can be easily verified by looking at the application logs or by using Wireshark.

Access Servers use an SSL server certificate signed using SHA-256 with RSA by a well-known Certification Authority.

Relay Server Connection

The End-to-end encryption securing remote access connections between Control Center and Runtime uses an AES-256 with a session key securely exchanged through a separate Access Server connection during the handshake phase. Since the Relay Server never participates to this handshake and is simply used after the session key has been exchanged, it cannot decode the incoming traffic and the connection is truly end-to-end secure.

The underlying transport is TCP (preferred for performance reasons) or TLS1.2 (as fallback for compatibility with firewalls requiring a TLS connection). Note that confidentiality is not guaranteed by TLS in this case, but by the upper-level AES-256 encapsulation.

Web API Connection

All Frontends use HTTPS for web APIs. Web servers use an SSL server certificate signed using SHA-256 with RSA by a well-known Certification Authority.

Remote access tools security

VPN

Once a Control Center or a Tools Applet client is connected to a Runtime client, a VPN connection can be established depending on how the “VPN access” permission is given to a user on a given device.

The UBIQUITY VPN works at level 2 of the ISO/OSI protocol stack, i.e., it encapsulates Ethernet frames instead of IP packets. This is done for best compatibility with common industrial scenarios, where non-IP protocols or broadcast messages are used.

The VPN is implemented by installing a virtual Ethernet adapter on the Frontend PC.

UBIQUITY Runtime can intercept low level network traffic of selected physical interfaces and channel it to the Frontend’s virtual Ethernet adapter. For both the Frontend machine and the UBIQUITY Runtime device, it appears as if the Frontend machine is physically connected to the selected Runtime LAN.

Even if level 2 is below IP, by default the Runtime service automatically assigns a free IP to the Frontend virtual VPN adapter. This is done by convenience, since most useful protocols are IP based and thus ready to work. Moreover, IPs from the actual physical subnet(s) are used. No virtual IP subnets and consequent routing rules are created.

The Runtime periodically polls for existing devices on the network by sending ARP messages. It discovers “free” IPs that can be later assigned to VPN connections. This policy is handy but can be changed if a stricter and more controlled configuration is needed.
An IP pool can be configured on the device so the Runtime will only assign IPs coming from this pool. In this case no ARP discovery is performed.

Having the Frontend PC virtually connected to the physical device network is very powerful and handy, but it can be configured and limited in several ways to comply with ICT policies.

VPN firewall rules can be configured in the UBIQUITY domain to control what kind of traffic of a certain combination of device/sub-device/user/protocol can be remotely used. These rules can be obtained by configuring firewall rules across the domain hierarchy. Rules are hierarchical, per-user, per-resource, or per-resource group and can be limited to a certain remote MAC address, remote IPs, subnets, Ethernet or IP protocols, in an ALLOW – DENY fashion.
The result set of rules are calculated by the server before a VPN connection starts and are enforced on both Frontend and Runtime.

The best practice security-wise is to only enable the protocols and reachable destination needed by a specific remote user or user group. This makes the VPN connection even more secure than an actual physical local connection, because in the latter case, the local PC firewall would be the only mechanism to limit traffic. In our case, the UBIQUITY infrastructure takes care of enforcing the security rules decided by the administrator.

File Transfer

Remote file operations (download, upload, rename, delete) are served through the UBIQUITY Service process. This process is running with local system privileges by default.
In any case, the UBIQUITY domain admin can enable or disable this operation for remote users depending on how the "File Transfer" permission is propagated to a certain device for a certain user.

Authentication

Authentication of Users to Servers

The users of UBIQUITY can log into the service with:

- Domain name
- Username
- Password

The UBIQUITY domain admins can enforce users to use a strong password by IEC 62443 standard. This enforces the following minimum requirements:

- Minimum 8 characters in length
- Contains at least 3 of the following items:
  - Uppercase Letters
  - Lowercase Letters
  - Numbers
  - Symbols
- Minimum 8 characters in length

Upon creating a new user by an admin, the user is required to change their password. It means that at any time, an admin can't login using a user's credentials without the user noticing (it would require setting a new password).

Two-Factor Authentication (2FA)

As an additional security measure, users can voluntarily – or enforced by the admin – use two-factor authentication (2FA).

UBIQUITY uses the Time-based One-Time Password algorithm (TOTP) adopted as Internet Engineering Task Force standard RFC 6238 and based on the HMAC-based One-time Password Algorithm published as an informational IETF RFC 4226.

It is compatible with Google Authenticator and most other two-factor authentication apps.

Authentication of Runtimes to Servers

When UBIQUITY Runtime connects to the Access Server for the first time, it obtains a signed identity filethat contains the device UID in the UBIQUITY Domain. The certificate is used for authenticating devices to the server and relies to the operating system file system security. The certificate file is only accessible by elevated processes.

UBIQUITY Routers use an additional hardware feature that ensures device binding to a certain domain. In UBIQUITY Routers the UID is written in the hardware during the production stage in the factory and cannot be changed.
Once the Router is registered to a UBIQUITY Domain, it cannot be registered to another domain until the legitimate domain admin deregisters it from their domain. This is made possible by correlating the actual device identity to the hardware UID. This way, even if an attacker obtains physical access to the Router and performs a factory reset to reconfigure it, they won’t be able to register it to their domain and thus use the Router for malicious remote access to the network.

Authentication of Access Servers to Frontends and Runtime

As mentioned, clients use TLS 1.2 for connecting to Access Servers. Access Servers use an SSL server certificate signed by a well-known Certification Authority. Clients can verify the signature against the Certification Authority certificates installed in the system.

Operation Audit

The UBIQUITY clients automatically record the operations performed on their domain resources by users (such as device removal, renaming, etc.) and send the information to the UBIQUITY domain. The audit log can be queried at any time by admins using Frontends and cannot be disabled or deleted, not even admins.

Each log holds:

- The user that performed the operation
- The operation code (such as rename of a device)
- The resource that was the object of the operation (e.g., a device)
- The timestamp
- A description

In more detail, the audit trail contains:

- Login/logout of users.
- All CRUD (create, rename, update, delete) operations performed on all domain resources:
    - Users
    - Groups
    - Permissions
    - Device

    - Configurations
- All remote access operations, with starting time and ending time.

In addition, the domain admin can *optionally* enable a full log of all operations performed during every remote access session including:

- Start/end times of remote-control sessions (view-only or interactive).
- Files transferred.
- Processes started and killed.
- Protocols, IPs and MACs contacted in a VPN session.

Authorization

UBIQUITY authorization model is similar to the Active Directory's one.

The customer's UBIQUITY domain contains all the domain resources: users, groups and devices.
The domain administrator can design the domain and its rules to map any kind of organizational structure. Specifically, new users and groups can be created to properly map the organization and make configuration easier and more scalable.
Policies and permission rules can be applied to single resources or folders to apply them in a hierarchical way.

Finally, the Web API and the Access Server will enforce types of operations (such as remote desktop or file transfer) that will be allowed for a certain user of a certain resource (such as remote device).

The UBIQUITY User Manual describes all the ways authorization rules can be configured.

Cyber-attacks Countermeasures

Brute force detection

After a few unsuccessfully login attempts, Access Server completely blocks the incoming public IP address for a few minutes.

This measure, plus the password minimum requirements, makes brute force password discovery attempts ineffective.

Password management

Passwords in the UBIQUITY domain are not stored in clear text form. They are rather stored in hash form using a one-way cryptographic key derivation function and a per-user salt. The hash + salt pair ensures that even in case of data theft, an attacker cannot calculate the actual password from the hash by brute force using techniques such as rainbow tables.

Code Signing

UBIQUITY application binaries are signed with a private key. This ensures that users can always validate the authenticity and integrity of UBIQUITY applications.

Man-in-the-middle

Access Server, Web APIs, and Frontend-Runtime connections all use end-to-end encryption (explained above) that make man-in-the-middle attacks not possible.

Datacenter

Security Standards

Access Servers, Database Servers and the Web API servers are hosted on Microsoft Azure.
Azure is certified for ISO/IEC 27001:2013 and other security standards and certifications. Please refer to the following pages:

https://www.microsoft.com/en-us/TrustCenter/Compliance/ISO-IEC-27001
https://azure.microsoft.com/en-us/overview/trusted-cloud/

UBIQUITY Relay Servers are hosted in heterogeneous and geographically spread locations to be statistically nearer either Frontend or Runtime in order to lower latency. However, because of the special UBIQUITY network architecture explained above, they cannot cause any availability or security issue. Specifically:

- Relay Servers are dynamically discovered. Even if a node is not available, clients will automatically switch to the others.
- Relay Servers are an intermediate hop of an end-to-end encrypted channel, explained above. A man-in-the-middle attack scenario is not possible.
- No data is stored on Relay Servers.

Backup

A SQL log backup is done continuously with a Point In Time Restore of 7 days. Backups are also geographically spread.

Software Updates

Updates of Control Center, Tools Applet, Runtime and device firmware containing the UBIQUITY software are published on a regular basis.

The updates can be either downloaded from the website and installed manually, or they can be installed by the Access Server *semi-automatically*.
In the latter case, a domain admin is still responsible for manually deciding what device to update and when (immediately or within a scheduled time frame). After giving instructions to the servers via Frontend, the updates will be delivered from the cloud as planned.

A fully automatic update function without user intervention is not available for security reasons, because UBIQUITY is meant to be installed and used in mission critical installations.

Data Breach Policy

A data breach generally refers to the unauthorized access and retrieval of information that may include corporate and / or personal data.

In this context, data breach regards access to UBIQUITY servers and its data.

The regulations across the various jurisdictions in which ASEM operates require ASEM to make reasonable security arrangements to protect the personal data that we possess or control, to prevent unauthorized access, collection, use, disclosure or similar risks.

Data breaches may be caused by employees, parties external to the organization, or computer system errors.

All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to:

- Investigate the failure and take remedial steps if necessary.
- Maintain a register of compliance failures.
- Notify the Supervisory Authority of any compliance failures that are material either in their own right or as part of a pattern of failures.

ASEM will notify any affected clients after becoming aware of a data breach. However, ASEM does not have to notify the data subjects if anonymized data is breached. Specifically, notifying data breach subjects is not required if the data controller has implemented techniques like encryption along with adequate technical and organizational protection measures to the personal data affected by the data breach.

Best Practices

- The UBIQUITY Domain should be configured to require strong user password per IEC 62443-3-3. Newly created domains have this option enabled by default. Refer to the User Manual for more information.
- Two-factor-authentication should be enforced by UBIQUITY Administrators for all users.
- In case of software installations on Windows machines, a firewall in the network (best if a hardware firewall) should be configured so that all connections from the Internet to the machine are blocked. Only one outgoing port should be used by UBIQUITY (TCP port 443, 80 or 5935) and kept open from the machine to the Internet
- Windows machines should only run controlled and safe software.
- The UBIQUITY software should be updated in case security improvements are released.
- Given the suggestions above, and given proper, static and controlled industrial environment, an antivirus software can be avoided.
- A strong administrator password change per IEC 62443-3-3 is enforced to register a Router to a domain. Please, keep the administrator password safe and do not share it with unauthorized personnel.
- UBIQUITY Routers can be connected to the Internet through its WAN port. UBIQUITY Routers don’t enable any service through that port and will only need an outgoing connection through to the configured outgoing port (TCP port 443, 80 or 5935). They basically don’t expose any surface to known attacks from the outside. We periodically test the latest version of the firmware stack against new kinds of attacks. However, for best security, an additional specialized firewall hardware would ensure the best protection from the outside.