Using Managed Certificate Whitelisting as a Basis for Internet of Things Security in Industrial Automation Applications

Rainer Falk and Steffen Fries
Siemens AG
Corporate Technology
Munich, Germany
Email: {rainer.falk|steffen.fries}@siemens.com

***Abstract*—Device authentication is a basic security feature for automation systems, and for the future Internet of Things. The design, setup, and operation of a practically usable security infrastructure for the management of required device credentials – as cryptographic device keys, and device certificates – is a huge challenge. Also, access permissions defining authorized communication peers have to be configured on devices. The setup, and operation of a public key infrastructure PKI with registration authority (RA), and certification authority (CA), as well as the management of device permissions has shown to be burdensome for industrial application domains. A recent approach is based on certificate whitelisting. It is currently standardized for field device communication within energy automation systems by IEC 62351 in alignment with ITU-T X.509. This new approach changes the way how digital certificates are used, and managed significantly. After describing the new approach of managed certificate whitelisting, and giving a summary of ongoing standardization activities, an example for the application in a real-world application domain is described. Needs for further technical work are derived, and solution options are presented.**

***Keywords*—Digital certificate; certificate whitelisting; credential management; PKI; device authentication; Internet of Things.**

I. Introduction

Industrial automation control systems (IACS) monitor, and control automation systems in different automation domains, e. g., energy automation, railway automation, or process automation. The main functionality can be summarized on a high level to performing control operations in the physical world using actuators, based on physical measurements obtained by sensors. Automation control systems are using open communication protocols like Ethernet, IP, TCP/UDP internally, and for communication with external systems (e. g., for monitoring, diagnosis, configuration), realizing an Internet of Things (IoT), or the Web of systems. The term "Internet of Things" commonly refers to a set of technologies supporting the connection of hitherto stand-alone devices to an IP-based network. These technologies are important enablers for the convergence of today's automation architectures with service-oriented approaches while meeting industry-grade safety, security, reliability, and real-time requirements.

In a common realization of a public key infrastructure PKI, digital certificates are issued by a trusted certification authority (CA). This allows to authenticate devices. Additionally, access permissions are defined for authorized communication peers. While this technology could be the basis for a global, uniform secure communication, in reality, the deployment, and adoption of PKIs is often limited to HTTP server authentication. A reason for that is the significant effort required to setup, maintain, and use a PKI. Also, differing interests of involved stakeholders prevent that a single security infrastructure can be setup that is relied upon by all stakeholders. The problem addressed in this paper is the practical management of device certificates for field-level automation devices, being an extended version of [1].

Industrial automation control systems use open communication protocols as Ethernet, wireless local area network (WLAN) IEEE 802.11 [2], transmission control protocol (TCP), user datagram protocol (UDP), and hypertext transfer protocol (HTTP) [3]. The communication can be protected using standard security protocols like IEEE 802.1X/MACsec [4], Internet key exchange (IKE) [5] with Internet protocol security (IPsec) [6], secure shell (ssh) [7], secure sockets layer (SSL) [8], and transport layer security (TLS) [9]. Often, asymmetric cryptographic keys, and corresponding device certificates are used. Symmetric keys would not scale well for the huge number of involved devices as pairwise shared secrets would need to be managed. This is be feasible only for a small number of devices.

A certificate infrastructure is required that is suitable for an operational automation environment. Main considerations are the demand for extremely high system availability, requiring that the automation system can continue to operate in an autonomous island mode, and the fact that many automation systems are setup as separate network segments that have no, or only limited connectivity with general office networks, or even the public Internet. Moreover, the fact that these systems are typically engineered, e.g., that the communication relations are known up front, can be leveraged for certificate and access management. It should also be mentioned that certification of products and solutions plays an increasingly important role. Especially in the area of critical infrastructures, regulatory requirements for product certification exist. But also operators require certified products to ensure both their own compliance with defined security procedures, and policies, as well as to ensure product interoperability, and security. The industrial security standard being investigated in this paper is ISO/IEC 62433 [10], which on one hand defines security levels, and on the other hand defines requirements

for each security level, without being prescriptive about the actual implementation. This standard is currently intended to enhance the industrial automation certification scheme of IEC IECEE [11] with respect to security.

Existing approaches for device certificate management have severe limitations when applied for field-level automation devices. A self-contained certificate management tool (command line tool, or with GUI) can be, with corresponding procedures, and personal, and organizational security measures, well suited for a small number of devices, but it does not scale well to scenarios with a larger number of devices. A full-blown PKI infrastructure could be efficient for an extremely huge number of devices, as, e. g., WiMax, or cellular modems, but these go beyond the scale of a common single automation systems.

The problem can be summarized that a solution is needed that can be setup, and operated autonomously within a certain automation environment without relying on a globally accepted certification authority, and that scales well for "mid-size" automation environments, for which a self-contained certificate tool is too small, and a full PKI solution would be too complex, and costly. It may be also advantageous to avoid the need for deploying a separate identity, and access management infrastructure. The paper is an extended version of [1] that presents in particular more details about security for industrial automation, and control systems, and describes extended example for the usage of certificate whitelisting within the energy automation application domain.

The remainder of this paper if structured as follows: After summarizing background work in Section II, an overview on the industrial security standards IEC62443 [10] is given in section III. Section IV describes certificate whitelists as a new paradigm for using digital certificates. The management of certificate whitelists is described generically in Section V, and a specific adaption into energy automation systems is outlined in Section VI. An outlook to possible future extensions is given in Section VII.

II. Background and Previous Work

Secure communication protocols, digital certificates, and public key infrastructure PKI [12], [13] have been dealt with intensively for years. An introduction is given in common text books on IT security [14]. The remainder of this section summarizes shortly major aspects that are relevant to managed certificate whitelists.

A. Device Communication Security Technologies

Digital device certificates are the basis for device communication security as used in industrial automation systems, and in the future Internet of Things (IoT). Major communication security protocols are available for the different layers of the communication protocol stack that support digital device certificates for authentication:

- Link layer: The standard 802.1X [4] provides Network Access Control to restrict access to a network only for authenticated devices. It is also possible to encrypt the communication link using the MACsec of 802.1X.

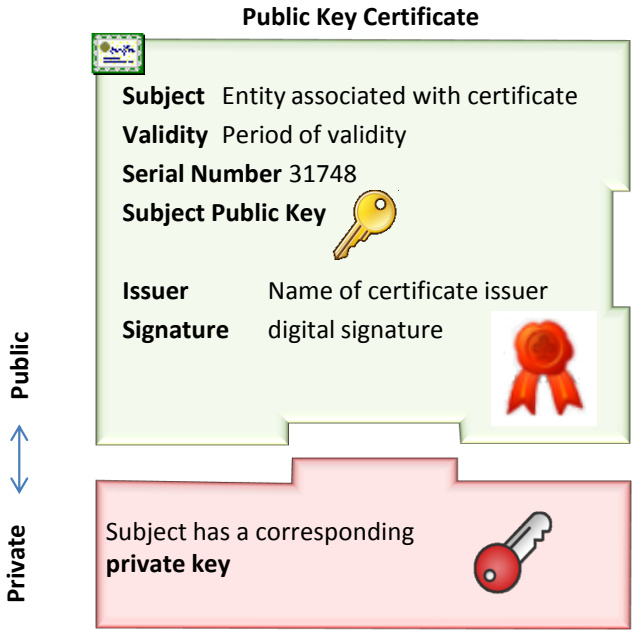

Fig. 1. Digital Certificate (X.509)

- Network layer: The communication can be protected with IPsec [6] on the network layer. The required security associations can be established by the IKE [5] protocol.
- Transport layer: With TLS [9], the successor of the SSL protocol [8], communication can be protected on the transport layer.
- Application layer: SSH, or WS-Sec are available to protect application layer protocols as HTTP, SOA (REST, SOAP), CoAP, XMPP, or MQTT.

B. Digital Certificates

The main purpose of a digital certificate is to reliably assign information about the subject, i. e., the owner, of a public key. The owner may be identified by its name, or email address in case of a person, or by its network name (DNS name), or IP address of a server. Additional information encodes usage information about the public key respectively the digital certificate, as validity period, and allowed key usages as user authentication, or email encryption. For device certificates, it is possible to encode the device manufacturer, the device model, and the serial number within a device certificate.

The most commonly used certificate format is ISO X.509 [12]. Figure 1 shows the format, and some exemplary fields. The main purpose of a digital certificate is to bind a public key (`Subject Public Key Info`) of an entity to the name of the entity (`Subject`). Additional information as the validity period, the issuer, and usage restrictions can be included as well. X.509 certificates also support extensions, so that specific information can be included in addition.

When a digital certificate of a subject is validated by a communication peer, it is verified that the certificate has a valid digital signature of a trusted certification authority. It is

furthermore verified that the entries of the certificate match the intended usage, and that the certificate has not yet expired. It may also be verified whether the certificate has been revoked. A revocation check, see also subsection II-D below, may verify whether a given certificate is included in a certificate revocation list (CRL), or an online revocation status check may be performed using the open certificate status protocol (OCSP) [15]. In either case, at least partial online access to a PKI entity that is issuing certificates, and providing revocation information is needed at least from one component in an automation network, or cell. This component may further distribute the information within the automation cell.

C. Certificate Root Key

A digital certificate has to be validated before it is accepted. This includes a check whether the digital signature protecting the certificate is trusted. The standard approach is to use a set of trusted root certificates for certification authorities CA. A certificate is accepted if its signature chain can be verified back to a trusted root certificate. The root certificate may belong to a globally recognized CA, or to a local CA that is accepted only within an administrative domain, e. g., within a single operator network. If no PKI with CA is available, it is also possible to use self-signed certificates. This means that each certificate is signed with the private key associated with the public key contained in the certificate. Such certificates have to be configured as trusted in the same way as trusted root certificates, i. e., the (self-signed) certificates of trusted peers have to be configured explicitly. This requires to store the trusted peer information (root CA, or self signed certificates) in a secure manner, as this information is crucial for system security. A potential attack is the inclusion of an untrusted root certificate in the list of root certificates managed by a device. This attack is not specific to field devices. Some operating systems and web browsers also feature a certificate store containing a variety of root certificates that could be compromised. If an adversary would be able to introduce a new untrusted certificate into this root certificate store, he would compromise the system. Hence, the certificate store or certificate list has to be protected.

D. Certificate Issuance and Revocation

A digital certificate is issued by a certification authority (CA) of the public key infrastructure (PKI). This means that the certification authority creates the signed certificate for an entity, protected by the digital signature of the CA. It is common that the request to issue a certificate is received, and checked by a registration authority (RA), separating the checking, and the cryptographic functionality. A request to issue a digital certificate is sent typically using a certificate signing request (CSR) [16], using the simple certificate enrollment protocol (SCEP) [17], or by using enrollment over secure transport (EST) [18].

In cases where no PKI can be setup, also self-signed certificates are used. Here, an entity creates its own certificate, and signs it. The self-signed certificates, or a hash values (fingerprints) of the certificate, have to be configured on peers. This is practical only for small environments, due to the involved administration effort.

For industrial environments, an approach is to use pre-installed manufacturer device certificates on devices. These can be used to securely configure operational device credentials, and to protect certificate requests for operational device certificate to be used during operation.

A digital certificate can be revoked by the issueing CA. The most common approach is to use a certificate revocation list (CRL). A CRL is issued by a CA, indicating all certificates that have been issued, and later revoked by the CA. The drawback is that the current CRL has to be downloaded from the CA regularly, and that the size of a CRL can grow to large sizes being well suited for resource-limited IoT devices. An alternative is to use the OCSP protocol [15] to check the revocation status of a single certificate. This approach has the drawback that online connectivity is required.

In industrial environments, also short-lived certificates are used. The time of validity is set to a short time period so that revocation checks can be omitted [19].

E. Certificate Whitelisting

The basic concept of certificate whitelists is well-known. The underlying idea is to enumerate explicitly all authorized certificates. A certificate is validated successfully only if it is contained in the certificate whitelist. The whitelist may contain the certificates directly, or reference the certificates by their serial number, and issuer, by the certificate fingerprint, or by the public key. The latter avoids issuing a new whitelist, when a certificate is updated.

Such a certificate whitelist can be considered, and used also as an access control list that contains the certificates of all authorized subjects. Without using specific certificate extensions to encode different types of access, the different operations cannot be distinguished directly, however. Different certificate whitelists would have to be defined for different types of access. The configuration of the set of trusted root certificates is also a form of certificate whitelists. It is known to check whether the certificate of a communication peer is included in a certificate whitelist [20]. Also, the Microsoft Digital Rights Management License Protocol is using a certificate whitelists [21].

As these certificate whitelists have been used as a proprietary means for configuring a list of trusted certificates, or to be more precise a *set* of trusted certificates, the approach has been rather limited as general means for certificate management.

Other examples can be given through the pinning of certificates, which is also often done using CWL-like list. In contrast to the CWL approach described in this paper, the "classical" pinning takes the certificate from the very first connection as secure. It merely ensures that connections established afterwards are always verified against the list of "first connection certificates". The protocol secure shell (SSH) [7] is an example for relying on this approach: The server key

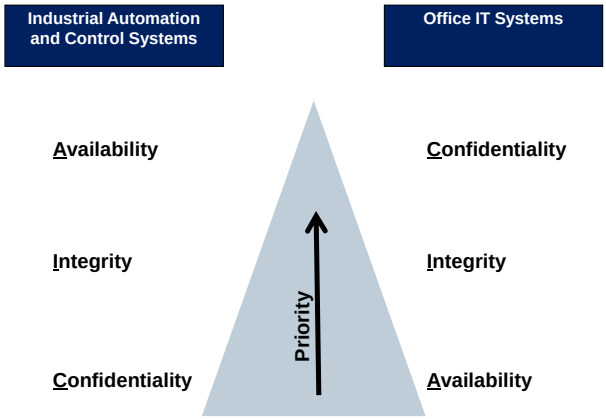

Fig. 2. Inverted CIA Pyramid

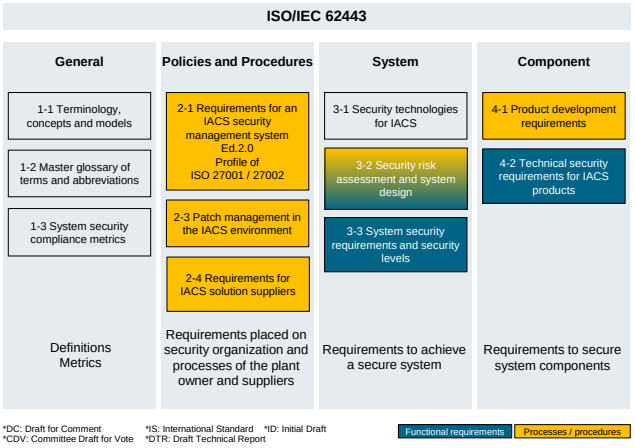

Fig. 3. Parts of ISO/IEC 62443

of the first connection is stored. There exist browser plug-ins that provide the same functionality for SSL/TLS-protected connections, like Certificate Patrol [22].

III. Security Standard IEC62443 for Industrial Automation Control Systems

Industrial automation control systems (IACS) monitor, and control automation systems in different automation domains. As networked automation control systems are exposed to external systems, they have to be protected against attacks to prevent manipulation of control operations. Krotofil and Gollmann have summarized research in the area of industrial control systems security [23]. Attacks have occurred in real world, see [24] reporting on a cyber attack where a steel mill could not be shut down correctly, causing severe damages.

The three basic security requirements are confidentiality, integrity, and availability. They are also named "CIA" requirements. Figure 2 shows that in common information technology (IT) systems, the priority is "CIA". However, in automation systems, also called operation technology (OT), or industrial IT, the priorities are just the other way round: Availability has typically the highest priority, followed by integrity. Confidentiality is often no strong requirement for control communication. Shown graphically, the CIA pyramid is inverted (turned upside down) in automation systems.

Specific requirements, and side conditions of industrial automation systems like high availability, planned configuration (engineering info), long life cycles, unattended operation, realtime operation, and communication, as well as safety requirements have to be considered when designing a security solution. The IT (information technology) security requirements defined in [10] can be mapped to different automation domains, including energy automation, railway automation, building automation, process automation, and others.

The security standard ISO/IEC 62443 [10] defines security for industrial automation control systems. Several parts have been finalized, or are currently in the process of being defined, see Fig. 3. The different parts cover common definitions, and metrics, requirements on setup of a security organization, and processes, defining technical requirements on a secure system, and to secure system components.

A complex automation system is structured into zones that are connected by so-called "conduits". For each zone, the targeted security level (SL) is derived from a threat and risk analysis. The threat and risk analysis evaluates the exposure of a zone to attacks as well as the criticality of assets of a zone. While IEC 62443-3-2 defines security levels, and zones for the secure system design, IEC 62443-3-3 describes the requirements to comply with a dedicated security level in an abstract way, not prescribing the actual implementation.

Four security levels have been defined, targeting different categories of attackes:

- SL1: Protection against casual, or coincidental violation
- SL2: Protection against intentional violation using simple means, low resources, generic skills, low motivation
- SL3: Protection against intentional violation using sophisticated means, moderate resources, IACS specific skills, moderate motivation
- SL4: Protection against intentional violation using sophisticated means, extended resources, IACS specific skills, high motivation

For each security level, IEC62443 part 3-3 defines a set of requirements. Seven foundational requirements group specific requirements of a certain category:

- FR 1 – Identification and authentication control
- FR 2 – Use control
- FR 3 – System integrity
- FR 4 – Data confidentiality
- FR 5 – Restricted data flow
- FR 6 – Timely response to events
- FR 7 – Resource availability

The security standard ISO/IEC62443 [10] part 3.3 states several requirements affecting device authentication under the

group FR1 "identification and authentication control". Some most relevant requirements are summarized here:

- SR1.2 — Software process and device identification and authentication: All devices, and software processes shall be possible to be identified, and authenticated. This requirement is relevant from security level SL2, and higher. While in SL2, group-, or role-based identification, and authentication is permitted, for SL3, and SL4, a unique identification, and authentication of devices is required.
- SR1.5 -– Authenticator management: Authenticators are credentials used to authenticate users, devices, or software processes. They have to be initialized, and refreshed. Initial authenticators shall be possible to be changed. The requirement is relevant for SL2, SL3, and SL4. For SL3, and SL4, a hardware mechanism is required to protect authenticators.
- SR1.8 -– Public key infrastructure (PKI) certificates: When a PKI is used, it shall be operated according to commonly accepted best practices, or public key certificates shall be obtained from an existing PKI. The requirement is relevant for SL2, SL3, and SL4.
- SR1.9 — Strength of public key authentication: When digital certificates are used, the certificate, the certificate path, and the certificate revocation status have to be checked. In SL3, and SL4, private keys have to be protected using a hardware-based mechanism.

These requirements have to be fulfilled while respecting side-conditions on high availability, and keeping safety-critical control networks closed. These imply that a control system should continue to operate locally, independently from any backend systems, or backend connectivity. Local emergency actions, as well as essential control functions shall not be hampered with by security mechanisms.

IV. Certificate Management and Validation Using Certificate Whitelists

The setup, and operation of a public key infrastructure has shown to require significant effort, and costs. This has been a limiting factor for the practical usage of public key cryptography. Ongoing standardization activities define the technological basis for simpler usage of public key cryptography for industrial automation environments, and the future Internet of Things.

While a certificate whitelist has been used so far as proprietary means for configuring some digital certificates as trusted, a certificate whitelists format is currently being standardized for the smart energy grid environment. It has been acknowledged that the application of certificate whitelists in restricted environments supports the long term administration of security parameters. Hence, standardizing the format is the next consequent step to ensure interoperability of different vendor products.

A certificate whitelist is a data structure containing respectively referencing a set of trusted, or authorized digital certificates. A certificate can be referenced by its serial number, and issuer, or by a fingerprint of the certificate (hash value). The certificate whitelist is signed using a whitelist root key of trust (WROT). A Certificate White List is also referenced as Certificate Authorization List, e. g., by the ITU-T X.509 group.

A certificate is validated successfully if it is contained in a corresponding certificate whitelist. Further checks on the contents of the certificate as the name of the subject, the certificate extensions, and the certificate signature are performed in the usual way.

Certificate whitelists can be used with certificates issued by a CA, or with self-signed certificates. A common technological basis is provided for smaller environments using self-signed certificates as well as environments using a PKI for issuing certificates. So, a smooth migration from self-signed certificates to a local PKI, and even towards global PKI is provided. Whitelists are advantageous also in the case when device certificates, having a very long validity period of, e. g., 30 years, are used. In this case, such a long-lived device certificate is accepted only if the certificate is valid, and if, in addition, it is included in a certificate whitelist.

A certificate can be revoked easily by *not* including it anymore in the certificate whitelist. This supports that the requirement SR1.9 of ISO/IEC62443 [10] part 3.3 is fulfilled, without having to rely on backend security servers that would be required for CRL-based or OCSP-based revocation checks. However, it is also possible to check the certification revocation status using certificate revocation lists [12], or using the online certificate status protocol OCSP [15] in addition.

1) Standardization Activities: Currently, ongoing standardization activities performed by the working group IEC TC 57 WG15, standardizing ISO/IEC 62351 [25] in alignment with ITU-T X.509 [12] define the usage of certificate whitelists for energy automation systems. Currently, a format is defined for a certificate whitelist. Figure 4 shows a recent proposal for a certificate whitelist. It is based on the format of a certificate revocation list CRL, but its assigned type (`CertificateWhiteList`) distinguishes it from a CRL. Also, the intended scope of a certificate whitelist is defined by a specific attribute `scope`. It allows a client to verify whether a certain certificate whitelist has in fact been intended for a specific purpose. For example, the IP addresses, or DNS names of devices for which the whitelist is intended to be used, can be included.

The target scope of a certificate whitelist can be explicitly encoded in a certificate whitelist. Therefore, a certificate whitelist cannot be used unintentionally for a different purpose as the intended purpose at time of compilation. Certificate whitelists can be compiled once during as part of engineering. Alternatively, end devices can pull a certificate whitelist from a whitelist certificate server in defined time intervals. The CWL can also be pushed to the field devices.

A digital certificate may be intended to be used only within a certificate whitelisting environment. To ensure that a certificate is in fact validated successfully only together with a corresponding whitelist, it is possible to include a corresponding extension in the certificate. The extension marks it explicitly

```
CertificateWhiteList  ::=  SEQUENCE  {
     tbsCertWhiteList     TBSCertWhiteList,
     signatureAlgorithm   AlgorithmIdentifier,
     signatureValue       BIT STRING
}

TBSCertWhiteList  ::=  SEQUENCE  {
   version      Version OPTIONAL,
                -- if present must be v1
   signature    AlgorithmIdentifier,
   issuer       Name,
   thisUpdate      Time,
   nextUpdate      Time OPTIONAL,

   scopedList      SEQUENCE OF SEQUENCE {
      scope        ScopeConstraints,
                   -- geographic,organizational
      authorizedCertificates    SEQUENCE OF SEQUENCE  {
         fingerprint     AlgorithmIdentifier, -- for FP creation
         certIdentifier::== CHOICE {
         serialCert      [0] CertificateSerialNumber,
         fingerprintCert [1] OCTET STRING -- FP of certificate
         fingerprintPK   [2] OCTET STRING -- FP of public key
   }

   certificateIssuer     Name OPTIONAL,
   cwlEntryRestriction   [0] EXPLICIT Extension OPTIONAL
                         -- further restrictions of cert. usage
   }
   }

   cwlExtensions [0] EXPLICIT Extensions OPTIONAL
                 {- for future use
}
```

Fig. 4. Certificate Whitelist Format [25]

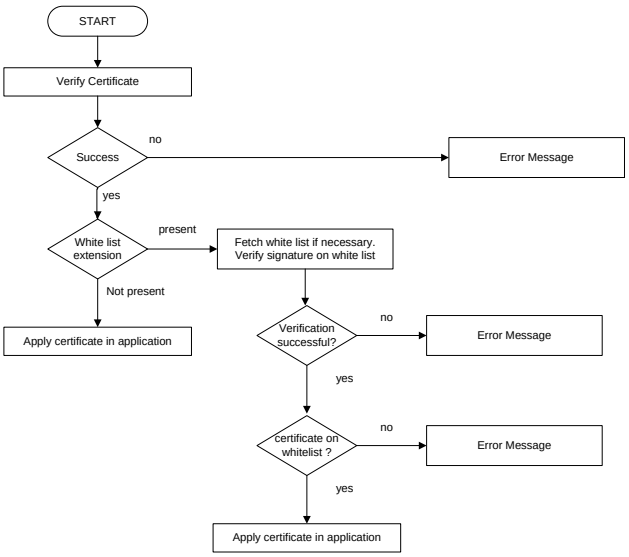

Fig. 5. Validation of a Certificate with Certificate Whitelisting

to be accepted only if it is included in a certificate whitelist. A corresponding certificate extension is currently defined in the scope of certificate management by ISO/IEC 62351 [25].

The validation of a certificate depends on whether it contains a certificate whitelist extension. Figure 5 shows the relevant checks. If a certificate includes the whitelisting extension, it is required that the corresponding whitelist is available, and that the certificate is in fact included in the whitelist.

V. Managed Certificate Whitelists

The introduction of certificate whitelisting implies the need for a management system for certificate whitelists. Managed certificate whitelists are a new approach for using public key cryptography in a practical, efficient, and effective way. It is particularly suited for systems with well-known set of devices, and their communication relationships, as it is common for networked automation systems. As the management of whitelists can be fully automated, it scales well to larger number of devices, although due to the increasing size of whitelists the targeted application environment is characterized by a number of devices within a range up to some 100 to some 1000 devices. It integrates well within existing industrial workflows for installing, or exchanging devices, as device configuration databases are kept up-to-date within automation systems. So, the information that is required to generate updated certificate whitelists is already available. Once certificate whitelists have been generated, and installed on the target devices, the target devices can operate autonomously even if the security infrastructure is not available. This is an important property for automation environments with high availability requirements to ensure that the automation system can continue to operate even if backend systems are temporarily unavailable.

A. Whitelist Generation and Distribution

The basic concept for automatic whitelist management is rather straightforward. Engineering information about the devices, and their communication relationships within a networked automation system is available in common automation systems. Several purpose-specific – and also device-specific if needed – certificate whitelists are generated automatically using this engineering information. The whitelists are distributed to the target devices using remote configuration protocols. For example, secure copy scp [7], HTTPS [26], or OPC-UA [27] can be used to distribute configuration files securely to the target devices.

Figure 6 shows the main components involved in the automatic management of certificate whitelists. A central device management component accesses a device database including all registered devices of a networked automation system, and their associated device certificates. Using automation system configuration data, the communication relationships are determined. This gives the list of the components installed in the automation system, and their communication links. Based on this information, certificate whitelists comprising the relevant certificates, can be compiled for the different communication purposes as automation control communication, supervisory control communication, remote service access, and diagnostic access. Depending on policy, device-specific certificate whitelists can be compiled, or certificate whitelists for defined purposes, and target device classes. The certificate whitelists are created, and provided to a device management system that configures the relevant certificate whitelists on the target devices. As important difference to a certification revocation list CRL, a certificate whitelist will usually be provided, and be signed by the operator, not by the certification authority

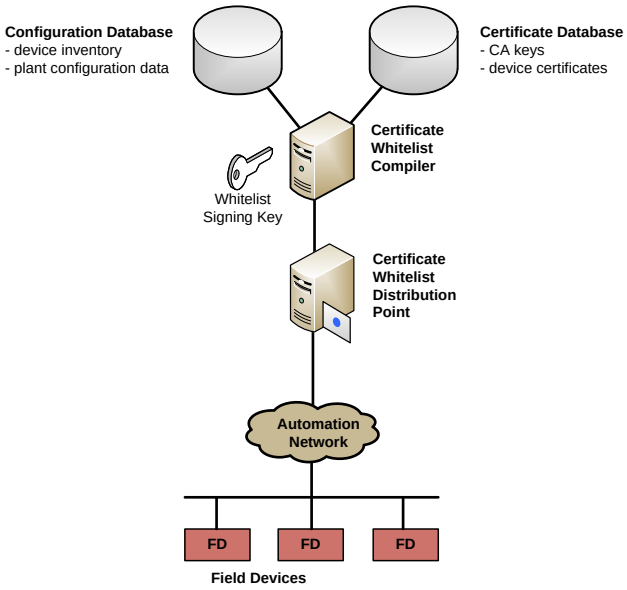

Fig. 6. Certificate Whitelist Management System

(CA). As the whitelist is a digitally signed data structure, the corresponding private key has to be protected, for example by using a smart card, or a hardware security module (HSM). However, note that while the digital certificates are signed usually by a certification authority (CA), the whitelist will by managed, and digitally signed, by the operator of the automation system. This has the advantage that an automation system operator can use managed certificate whitelists easily with certificates issued by different CAs, and even with long-lived, or self-signed certificates.

For networked automation systems with a typical size of some 100 to some 1000 devices, such a certificate management system based on whitelisting provides several advantages for the application in real-world industrial usage scenarios: A local PKI, long-lived, or even self-signed certificates can be used, so that a deployment with a very limited security infrastructure is possible. For the operation of the automation system, no continous reachability, or availability of the whitelisting security infrastructure is required. So, the availability of the automation system availability does not depend on the availability of the security infrastructure. A commonly availably device management infrastructure can be extended easily for automatically creating, and distributing certificate whitelists. It is possible to use a certificate whitelist only for authentication. Authorization checks would then be performed in addition, e. g., by checking an access control list. However, a certificate whitelist can be used directly as access control list as well. Different certificate whitelists would be configured for the different types of access (e. g., control communication, service access, diagnosis). The current proposal for a CWL structure considers this by supporting the encoding of a list of lists. Moreover, within the CWL, further certificate usage restrictions may be encoded. One example is the definition of dedicated applications, or communication protocols, which are allowed to utilize a dedicated certificate. Using this approach, the communication peer could refuse to accept a certificate included on the CWL if it is not associated within the CWL with the currently used communication protocol.

This approach has the advantage that no separate identity, and access management infrastructure is needed, and that access control decisions can be performed by a field device when the backend systems are not available. These properties make certificate whitelisting a very interesting approach for managing digital certificates in typical industrial automation systems.

B. Example Usage Scenarios

Typical workflows in industrial automation systems are the initial installation, the replacement, and removal of devices. As device configuration databases are already maintained as part of these workflows, the information for updating certificate whitelists is available without any extra effort required from the service personnel.

The certificate whitelist management system is triggered by a change in the configuration database. When a change in the configuration has been detected by the certificate whitelisting system, the generation of updated certificate whitelists is started. This happens preferably when a service mode of the automation system is terminated. The generated certificate whitelists are deployed automatically on the affected target devices using remote service access protocol, e. g., HTTPS [26], scp [7], or OPC-UA [27].

VI. Application Within Energy Automation Systems

The general approach of using managed certificate whitelists as described in the previous section can be applied for energy automation systems (smart grid). Figure 7 shows a substation automation system. A substation typically transforms voltage levels, and includes power monitoring, and protection functions. Figure 7 shows separate network zones of the substation communication network. The field devices that perform the actual field level functionality of monitoring, and acting on the electric power are called intelligent energy devices (IED). They are monitored, and controlled by a substation controller, realizing a realtime automation system. Energy automation protocols are defined by the standard IEC 61850 [28] which specified the Generic Object Oriented Substation Events (GOOSE) protocol, realizing the realtime communication with transfer requirements smaller than microseconds by utilizing multicast Ethernet connections between the field devices. Additional network zones are available for local, and remote service access, for integrating intelligent field devices with serial interfaces, and for support functions (file server, historian server for logging, remote access server, terminal server). A substation is connected to the utility communication network providing backend services like supervisory control, and data

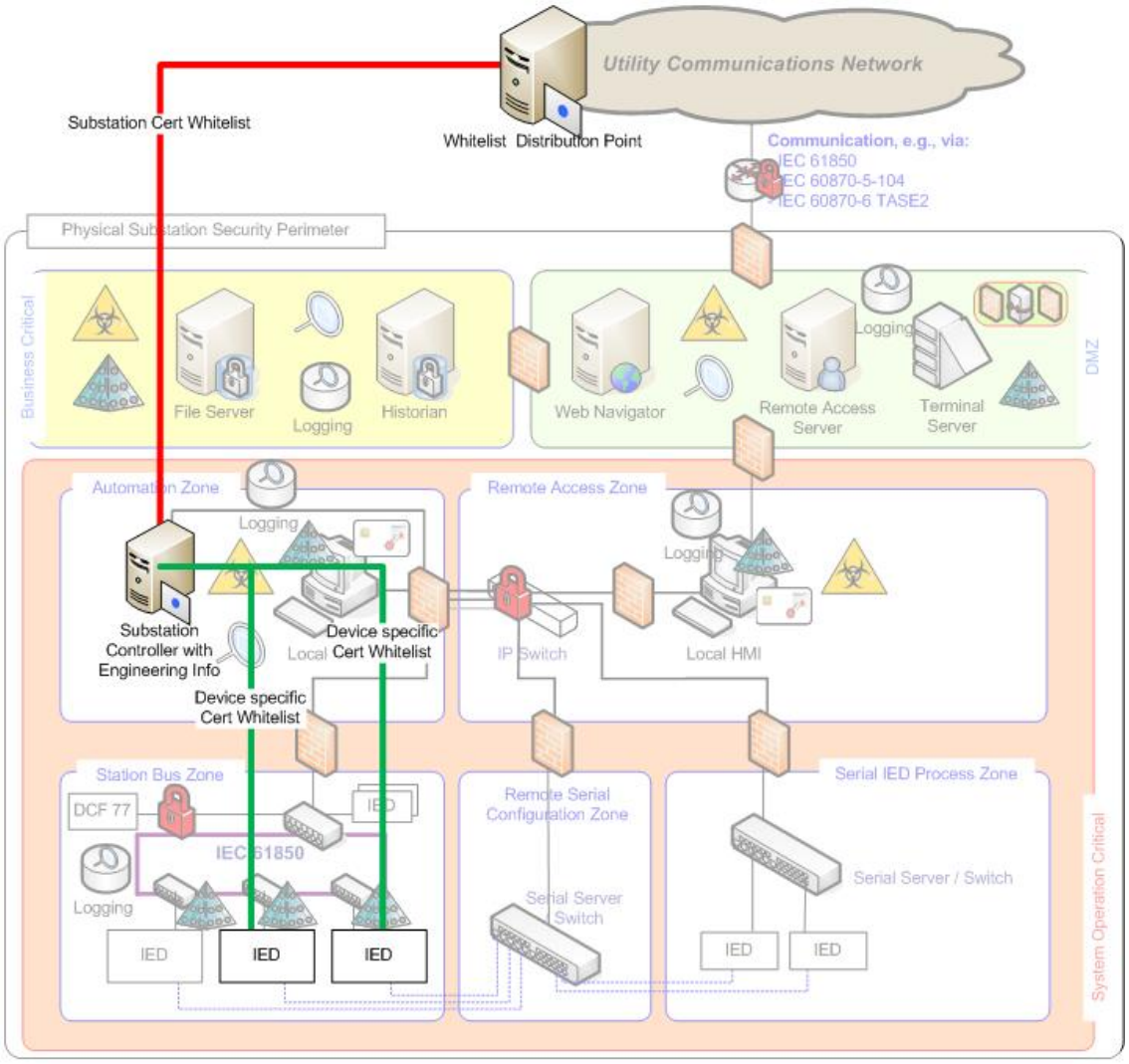

Fig. 7. Managed Certificate Whitelisting in Energy Automation Substations

acquisition (SCADA). Firewalls are used to control the traffic flow between zones.

A hierarchical creation, and distribution of certificate whitelists to a substation may be realized in the following way: A utility operator creates a substation-specific certificate whitelist (substation cert whitelist) based on the engineering information for this substation, and distributes it to the substation controller. This certificate whitelist contains the subset of certificates that are relevant for the substation. The specific substation is encoded in the CWL by the scope restriction. Using engineering information that is available at the substation controller, the substation controller creates device-specific certificate whitelists for the field devices, i. e., intelligent energy devices (IED), of the substation. The device-specific certificate whitelists are configured by the substation controller on the different IEDs.

An alternative approach would be to compile a CWL for a substation, and to distribute this CWL to all components in the substation via the substation controller. Through the engineering information, each IED will only communicate with other IEDs by means of the engineering data, and the CWL. This means that the access control decision is made by an IED by checking both the CWL, and the engineering information. This saves the additional effort for creating device specific CWLs, but has the disadvantage that each IED needs to search a larger CWL, and has to check two pieces of configuration information separately. It is a validation perfomance decision which approach is more appropriate in a target environment. The generic definition of CWLs allows for both approaches.

A further usage scenario for certificate whitelisting within energy automation systems would be the integration of decentralized energy resources. Here, a smart grid operator may realize a (managed) certificate pinning by using certificate whitelists. A smart grid operator would define which certificates are acceptable by including these certificates in a whitelist. Thereby, the smart grid operator would use certifi-

cate whitelists to restrict the set of certificates issued by a larger PKI. The possibility to misuse broken certificates, or CAs is reduced as the set of accepted certificates is limited.

VII. Conclusion and Outlook

Industrial automation control systems (IACS) monitor, and control automation systems in different automation domains, e. g., energy automation, railway automation, or process automation. As networked automation control systems are exposed not only to local attacks, but also to attacks originating from external systems, they have to be protected against attacks to prevent manipulation of control operations. Security requirements for automation systems have been defined by the industrial security standard ISO/IEC62443 [10], distinguishing four security levels.

The automation communication can often be protected using standard security protocols. Asymmetric cryptographic keys, and corresponding device certificates are used as symmetric keys would not scale well for the huge number of involved devices. Main considerations are the demand for extremely high system availability, requiring that the automation system can continue to operate in an autonomous island mode, and the fact that many automation systems are setup as separate network segments that have no, or only limited connectivity with general office networks, or even the public Internet.

This paper described a new approach for the practical management of device certificates for field-level automation devices, based on certificate whitelists. The fact that automation systems are typically engineered, e.g., that the communication relations are known up front, can be leveraged for automated certificate and access management. The basic concept of certificate whitelists is well-known. The underlying idea is to enumerate explicitly all authorized certificates. A certificate is validated successfully only if it is contained in the certificate whitelist. The whitelist may contain the certificates directly, or reference the certificates by their serial number, and issuer, by the certificate fingerprint, or by the public key. Such a certificate whitelist can be considered, and used also as an access control list that contains the certificates of all authorized subjects. Without using specific certificate extensions to encode different types of access, the different operations cannot be distinguished directly, however. Different certificate whitelists would have to be defined for different types of access.

Explicitly designating trusted certificates in certificate whitelists has been recently put forward within standardization for industrial energy automation communication [25]. It promises to provide a cost-efficient, easily deployable, and operable approach for digital device certificates even if self-signed certificates are used. It is intended for mid-sized industrial automation domains, while providing a migration path to more flexible PKI, and access management structures. It allows in particular to avoid the usage of simple manually configured pre-shared secrets, which would be difficult to migrate to more complex, and managed security infrastructures that are expected to be advantageous for large scale deployments. Its application is beneficial also in other industrial automation domains, e. g., railway automation, where very high availability requirements have to be fulfilled. Certificate whitelisting enables that a local control system can continue to operate autonomously when backend systems are not accessible for a certain time. They provide a way to fulfill the requirement for certificate revocation check, posed by industrial security standard ISO/IEC 62443 part 3.3 [10] independently from backend security servers (e. g., servers for identity, and access management, distribution points for certificate revocation lists, or online certificate status servers).

The usage of certificate whitelisting can be supported with automatic whitelist generation, and distribution. A format for certificate whitelists is currently proposed for standardization in ITU-T X.509, and for application in ISO/IEC 62351 in the context of key management in power automation. Specific extensions can mark a certificate explicitly for being used only in combination with a certificate whitelist.

Several additional extensions may be introduced in the future. It is possible to indicate usage restrictions within a certificate whitelist associated with a certain certificate entry. This could be used to limit the authorized usage of a certificate on a certificate-by-certificate basis. Certificate whitelists may be encoded efficiently by including matching criteria of included certificates. Alternatively to the explicit enumeration of certificates, a filter can be included in a certificate whitelist that defines matching criteria of included certificates, i. e., that defines required properties of certificate fields. A Bloom filter [29] may be used, combined with a check on false match. Bloom filters are a probabilistic data structure for membership queries which allow for an efficient encoding, but for which a wrong positive match may occur. As the set of all issued certificates is known in typical usage scenarios, a checking for a false match is easily possible. Also, certificates can be designated within a whitelist. Also, a PKI gateway can be deployed for secure interworking with external network domains using a standard public key infrastructure.

Also, the logical combination of multiple certificate whitelists is possible in general. The general concept of structured definition of access control policies by logically combining partial access control policies has been described, e. g., by [30]. A combination of certificate whitelists may be advantageous for instance in an inter-substation communication scenario. Here, a first certificate whitelist may be provided for the substation internal communication, and a second one for inter-substation communication. The final certificate whitelist for each purpose may be defined by a logical combination of whitelists to ease the certificate whitelist administration, and the handling for the field device. This might be done by logical OR, AND, or XOR combinations of the certificate whitelists. This logical combination can be realized in different ways: The field devices themselves can check against multiple certificate whitelists. A logical expression is configured that defines the logical combination of the certificate whitelists to be applied. As the defined certificate whitelist structure shown in Fig. 4 allows the encapsulation of multiple certificate

whitelists within a single data structure, an enhancement of this data structure could indicate the logical combination of the whitelist entries using the extension option.

A further alternative would be the preparation of device specific certificate whitelists by a centralized infrastructure component that determines the result of the logical combination of different certificate whitelists before distributing the actual certificate whitelist to the end points. This puts more effort on the centralized component, but keeps the effort low for the field device. The assumption here is that the certificate whitelist for a single endpoint is rather short compared to substation wide certificate whitelists containing all allowed (engineered) combinations of communication associations.

The structure defined in Fig. 4 also allows using different matching criteria for the certificate. While the serial number, and issuer, or the fingerprint are straight forward, the utilization of the public key fingerprint provides another degree of freedom. This approach allows even for updating certificates (assumed the public key stays the same) without changing the CWL. This decouples the certificate life cycle management from the access security policy management of certificates in automation environments.

References

[1] R. Falk and S. Fries, "Managed Certificate Whitelisting – A Basis for Internet of Things Security in Industrial Automation Applications," in *Proceedings of the 8th International Conference on Emerging Security Information, Systems and Technologies (SECURWARE), November 16–20, 2014, Lisbon, Portugal*. ThinkMind, Nov. 2014, pp. 167–172.

[2] IEEE 802.11, "IEEE Standard for Information Technology–Telecommunications and Information Exchange Between Systems, Local and Metropolitan Area Networks–Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications." [Online]. Available: http://standards.ieee.org/about/get/802/802.11.html [accessed: 2015-01-20]

[3] R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, and T. Barners-Lee, "Hypertext Transfer Protocol – HTTP/1.1," 1999, Internet Request for Comments RFC2696. [Online]. Available: https://tools.ietf.org/html/rfc2696 [accessed: 2015-01-20]

[4] IEEE 802.1X-2010, "IEEE Standard for Local and metropolitan area networks–Port-Based Network Access Control," . [Online]. Available: http://standards.ieee.org/findstds/standard/802.1X-2010.html [accessed: 2015-01-20]

[5] C. Kaufmann, P. Hoffman, Y. Nir, and P. Eronen, "Internet Key Exchange Protocol Version 2 (IKEv2)," Sep. 2010, Internet Request for Comments RFC5996. [Online]. Available: https://tools.ietf.org/html/rfc5996 [accessed: 2015-01-20

[6] S. Kent, and K. Seo, "Security Architecture for the Internet Protocol," Dec. 2005, Internet Request for Comments RFC4301. [Online]. Available: https://tools.ietf.org/html/rfc4301 [accessed: 2015-01-20]

[7] T. Ylonen, and C. Lonvick, "The Secure Shell (SSH) Protocol Architecture," Jan. 2006, Internet Request for Comments RFC4251. [Online]. Available: https://tools.ietf.org/html/rfc4251 [accessed: 2015-01-20]

[8] Netscape, "SSL 3.0 specification," Nov. 1996. [Online]. Available: http://web.archive.org/web/20080208141212/http://wp.netscape.com/eng/ssl3/ [accessed: 2015-01-20]

[9] T. Dierks, and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2," Aug. 2008, Internet Request for Comments RFC5246. [Online]. Available: https://tools.ietf.org/html/rfc5246 [accessed: 2015-01-20]

[10] ISO/IEC 62443, "Industrial Communication Networks -– Network and System Security," 2014, IEC TC57. [Online]. Available: [accessed: 2015-01-20]

[11] IEC IECEE, "IEC System of Conformity Assessment Schemes for Electrotechnical Equipment and Components (IECEE)," 2015, . [Online]. Available: http://www.iecee.org/ [accessed: 2015-01-20]

[12] ITU-T X.509, "X.509 Information technology – Open Systems Interconnection -– The Directory: Public-key and attribute certificate frameworks," 2012, version 3 corrigendum 3. [Online]. Available: http://www.itu.int/rec/T-REC-X.509-201210-S!Cor3/en [accessed: 2015-01-20]

[13] D. Cooper, S. Santesson, S. Farrel, S. Boeyen, R. Housley, and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile," May 2008, Internet Request for Comments RFC5280. [Online]. Available: https://tools.ietf.org/html/rfc5280 [accessed: 2015-01-20

[14] J. Buchmann, E. Karatsiolis, and A. Wiesmaier, "Introduction to Public Key Infrastructures," 2013.

[15] S. Santesson, M. Myers, R. Ankney, A. Malpani, S. Galperin, and C. Adams, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP," Jan. 2013, Internet Request for Comments RFC6960. [Online]. Available: https://tools.ietf.org/html/rfc6960 [accessed: 2015-01-20]

[16] M. Nystrom, and B. Kaliski, "PKCS #10: Certification Request Syntax Specification Version 1.7," Nov. 2000, Internet Request for Comments RFC2986. [Online]. Available: https://tools.ietf.org/html/rfc2986 [accessed: 2015-01-20

[17] M. Pritikin, A. Nourse, and J. Vilhuber, "Simple Certificate Enrollment Protocol ," Sep. 2011, Internet Draft draft-nourse-scep-2 (work in progress). [Online]. Available: http://tools.ietf.org/html/draft-nourse-scep-23 [accessed: 2015-01-20

[18] M. Pritikin, P. Yee, and D. Harkins, "Enrollment over Secure Transport," Oct. 2013, Internet Request for Comments RFC7030. [Online]. Available: https://tools.ietf.org/html/rfc7030 [accessed: 2015-01-20

[19] S. Fries and R. Falk, "Securely connecting Electric Vehicles to the Smart Grid," *International Journal On Advances in Internet Technology*, vol. 6, no. 1 and 2, pp. 57–67, 2013, ISSN: 1942-2652.

[20] eTutorials.org, "C/C++ Secure Programming – Chapter 10.9 Using a Whitelist to Verify Certificates," 2014, eTutorials.org. [Online]. Available: http://etutorials.org/Programming/secure+programming/ [accessed: 2015-01-20]

[21] Microsoft, "Digital Rights Management License Protocol – Retrieving Revocation Data from the Enrollment Server," 2014. [Online]. Available: http://msdn.microsoft.com/en-us/library/dd644914.aspx [accessed: 2015-01-20]

[22] CertPatrol, "Certificate Patrol 2.0," 2015. [Online]. Available: http://patrol.psyced.org/ [accessed: 2015-01-20]

[23] M. Krotofil and D. Gollmann, "Industrial Control Systems Security: What is Happening?" in *Proceedings of the 11th IEEE International Conference on Industrial Informatics (INDIN), 29-31 July 2013, Bochum*. IEEE, Jul. 2013.

[24] heise news, "BSI-Sicherheitsbericht: Erfolgreiche Cyber-Attacke auf deutsches Stahlwerk," 2014. [Online]. Available: http://www.heise.de/newsticker/meldung/BSI-Sicherheitsbericht-Erfolgreiche-Cyber-Attacke-auf-deutsches-Stahlwerk-2498990.html?view=print [accessed: 2015-01-20]

[25] ISO/IEC 62351, "Power Systems Management and Associated Information Exchange Data and Communication Security," 2014, IEC TC57. [Online]. Available: http://tc57.iec.ch/index-tc57.html [accessed: 2015-01-20]

[26] E. Rescorla, "HTTP Over TLS," 2000, Internet Request for Comments RFC2818. [Online]. Available: https://tools.ietf.org/html/rfc2818 [accessed: 2015-01-20]

[27] OPC Foundation, "OPC Unified Architecture Specification Part 1: Overview and Concepts, Release 1.02," Jul. 2012. [Online]. Available: http://www.opcfoundation.org/ua/ [accessed: 2015-01-20]

[28] ISO/IEC 61850, "IED Communications and Associated Data Models in Power Systems," 2014, IEC TC57. [Online]. Available: http://tc57.iec.ch/index-tc57.html [accessed: 2015-01-20]

[29] Wikipedia, "Bloom Filter." [Online]. Available: http://en.wikipedia.org/wiki/Bloom_filter [accessed: 2015-01-20]

[30] R. Falk, "A Method for Administering Access Rights in IT Systems [German: Eine Methode für die Verwaltung von Zugriffsrechten in IT-Systemen]," 2000, Dissertation, TU München.