Institut für Steuerungs- und Regelungssysteme
Professur für Vernetzte Sichere Automatisierungstechnik
Univ.-Prof. Dr.-Ing. Mike Barth
Fritz-Haber-Weg 1 (Geb. 30.33), 76131 Karlsruhe

CTRL + ALT + DEL PKI: Applicability of Certificateless Security

(Bachelor- or) Masterthesis

Public key infrastructures are a fundamental component of the security architecture of the Internet and, in the future, of industrial plants as well. But how transferable are alternative approaches to industrial plants?

Motivation

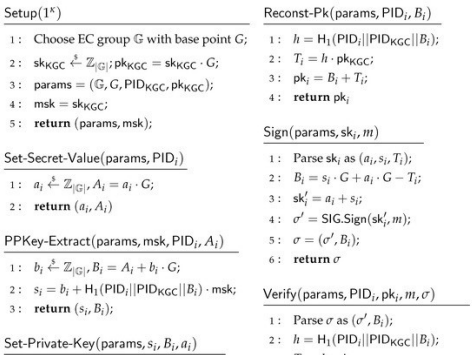
Public Key Infrastructures (PKIs) have long been the backbone of secure communication in the digital world. From secure websites to encrypted emails, PKIs enable trust through certificate-based authentication. However, as industrial environments continue to embrace digitization, automation, and connectivity, the adoption of PKI-based systems raises new challenges. Industrial plants (as in Figure 1) often feature long-lived devices, constrained hardware, legacy protocols, and limited connectivity - conditions not ideally suited for traditional certificate-based infrastructures.

Meanwhile, the complexity and maintenance overhead of PKI (certificate issuance, revocation, and renewal) are increasingly being questioned, especially in environments where uptime, determinism, and minimal human intervention are key. This leads to a provocative question: Can we hit CTRL + ALT + DEL on PKI — and reboot trust using alternative, certificateless security models like presented in Figure 2?

Figure 1: Industrial Modules

Goals

- Analyze certificateless cryptographic approaches (e.g., Identity-Based Encryption, Certificate-less Public Key Cryptography, ...), including their security properties, trust models, and deployment requirements
- Evaluate applicability and feasibility of these approaches in industrial environments, considering practical constraints such as device capabilities, lifecycle management, and interoperability.
- Develop a conceptual integration model or prototype, if feasible, to illustrate how certificateless security could be implemented in a representative industrial use case.



Setup(1^κ)
1: Choose EC group $\mathbb{G}$ with base point G;
2: $\mathsf{sk}_{\mathsf{KGC}} \xleftarrow{\$} \mathbb{Z}_{|\mathbb{G}|}$; $\mathsf{pk}_{\mathsf{KGC}} = \mathsf{sk}_{\mathsf{KGC}} \cdot G$;
3: $\mathsf{params} = (\mathbb{G}, G, \mathsf{PID}_{\mathsf{KGC}}, \mathsf{pk}_{\mathsf{KGC}})$;
4: $\mathsf{msk} = \mathsf{sk}_{\mathsf{KGC}}$;
5: **return** (params, msk);

Set-Secret-Value(params, PID_i)
1: $a_i \xleftarrow{\$} \mathbb{Z}_{|\mathbb{G}|}$, $A_i = a_i \cdot G$;
2: **return** (a_i, A_i)

PPKey-Extract(params, msk, PID_i, A_i)
1: $b_i \xleftarrow{\$} \mathbb{Z}_{|\mathbb{G}|}$, $B_i = A_i + b_i \cdot G$;
2: $s_i = b_i + \mathsf{H}_1(\mathsf{PID}_i||\mathsf{PID}_{\mathsf{KGC}}||B_i) \cdot \mathsf{msk}$;
3: **return** (s_i, B_i);

Set-Private-Key(params, s_i, B_i, a_i)

Reconst-Pk(params, PID_i, B_i)
1: $h = \mathsf{H}_1(\mathsf{PID}_i||\mathsf{PID}_{\mathsf{KGC}}||B_i)$;
2: $T_i = h \cdot \mathsf{pk}_{\mathsf{KGC}}$;
3: $\mathsf{pk}_i = B_i + T_i$;
4: **return** pk_i

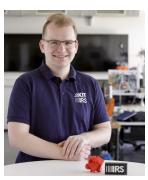
Sign(params, sk_i, m)
1: Parse sk_i as (a_i, s_i, T_i);
2: $B_i = s_i \cdot G + a_i \cdot G - T_i$;
3: $\mathsf{sk}'_i = a_i + s_i$;
4: $\sigma' = \mathsf{SIG.Sign}(\mathsf{sk}'_i, m)$;
5: $\sigma = (\sigma', B_i)$;
6: **return** σ

Verify(params, PID_i, pk_i, m, σ)
1: Parse σ as (σ', B_i);
2: $h = \mathsf{H}_1(\mathsf{PID}_i||\mathsf{PID}_{\mathsf{KGC}}||B_i)$;

Figure 2: Certificateless Cryptography

Interests and Helpful Prior Knowledge

- Interest in Cryptography and Security Concepts
- Basic Knowledge of Industrial Control Systems or the Ambition To Catch Up
- Lecture Information and Automation Technology



Supervisor
Marwin Madsen, M. Sc.
Build. 30.33, Room 110
Phone: 0721/608-42642
marwin.madsen@kit.edu

Thesis: (Bachelor or) Master
Date of Announcement: 08.08.2025
Tags: *Security, Industrial Control Systems, Certificate-less Public Key Cryptography*