CERIAS

The Center for Education and Research in Information Assurance and Security

Software Signing: Practical Adoption, Challenges, and Tooling Usability

Kelechi G. Kalu, Santiago Torres-Arias, James C. Davis

Software Signing Industrial Adoption and Challenges

An industry interview study of software signing for supply chain security.
Proceedings of the **34th USENIX Security Symposium (USENIX Security 25)**.

Software Signing Tooling Usability Analysis

Why Johnny Signs with Sigstore: Examining Tooling as a Factor in Software Signing Adoption in the Sigstore Ecosystem **(Under Review).**

Background, Motivation & Problem Statement

Background: How Software Signing Works

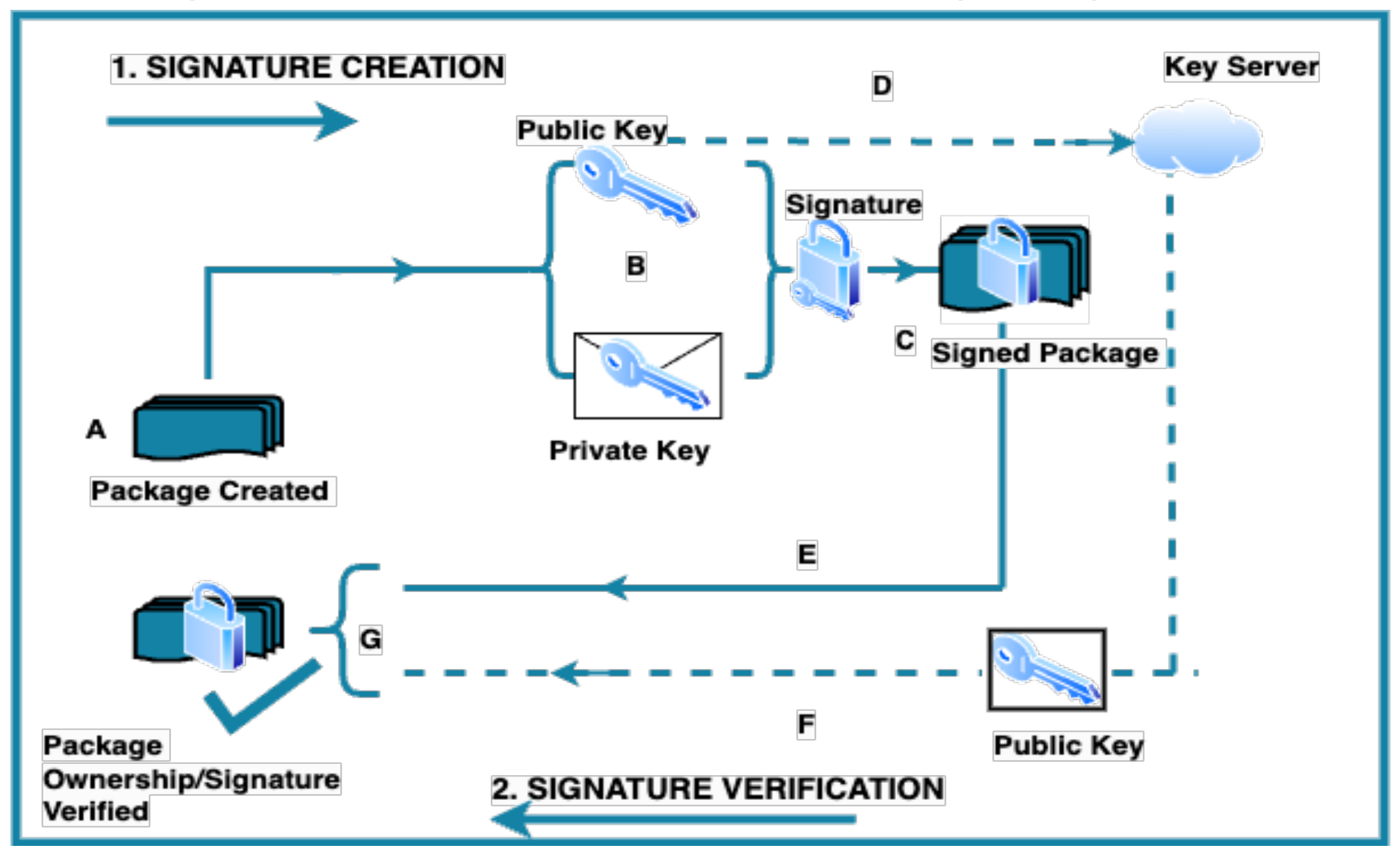


Figure 1. A typical software signing workflow.

Motivation: State of Software Signing

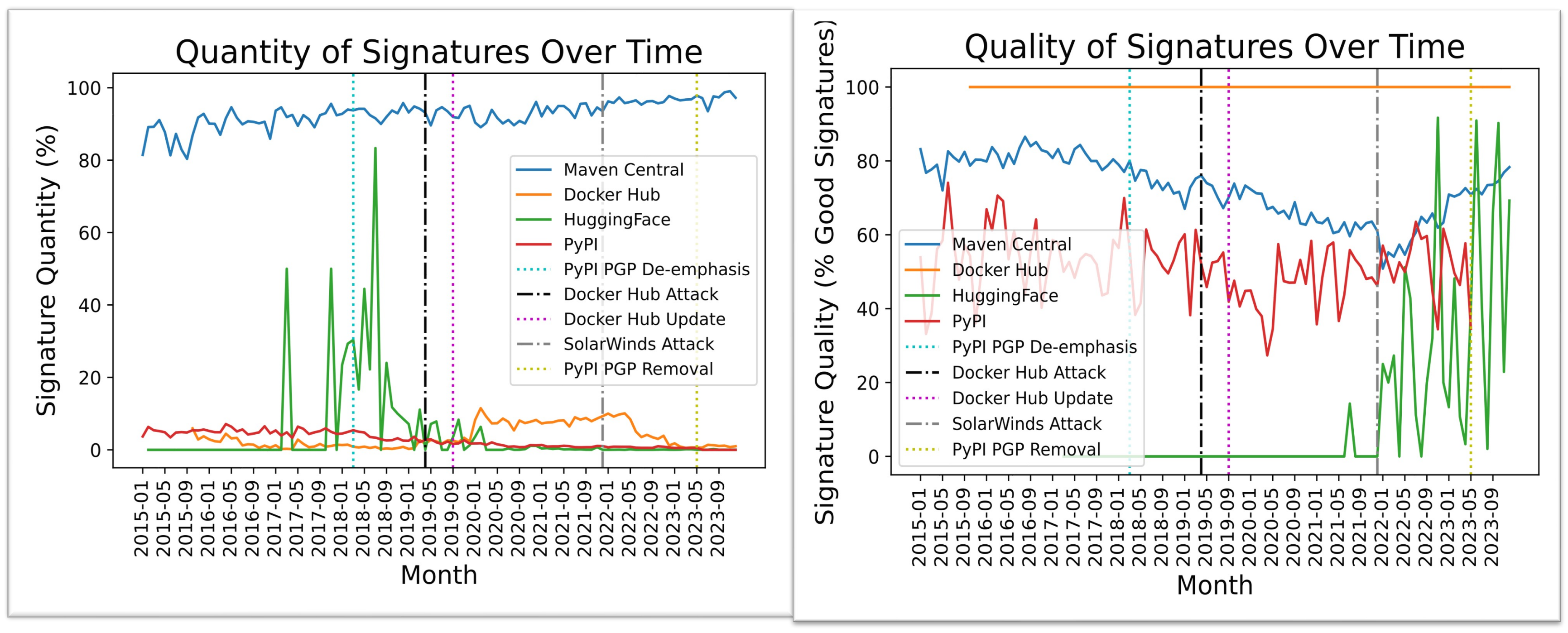


Figure 2. Schorlemmer etal's [1] software signature measurement study (IEEE S&P 2024): open-source packages are mostly unsigned, and the percentage of good quality signature mostly fluctuates.

Problem Statement

1. What are the software signing practices employed in industry?
2. Challenges to software signing in practice.
3. Usability evaluation of current software signing tools.

Methodology

- ❖ Qualitative Interviews - N = 18
- ❖ Framework and Thematic Analysis

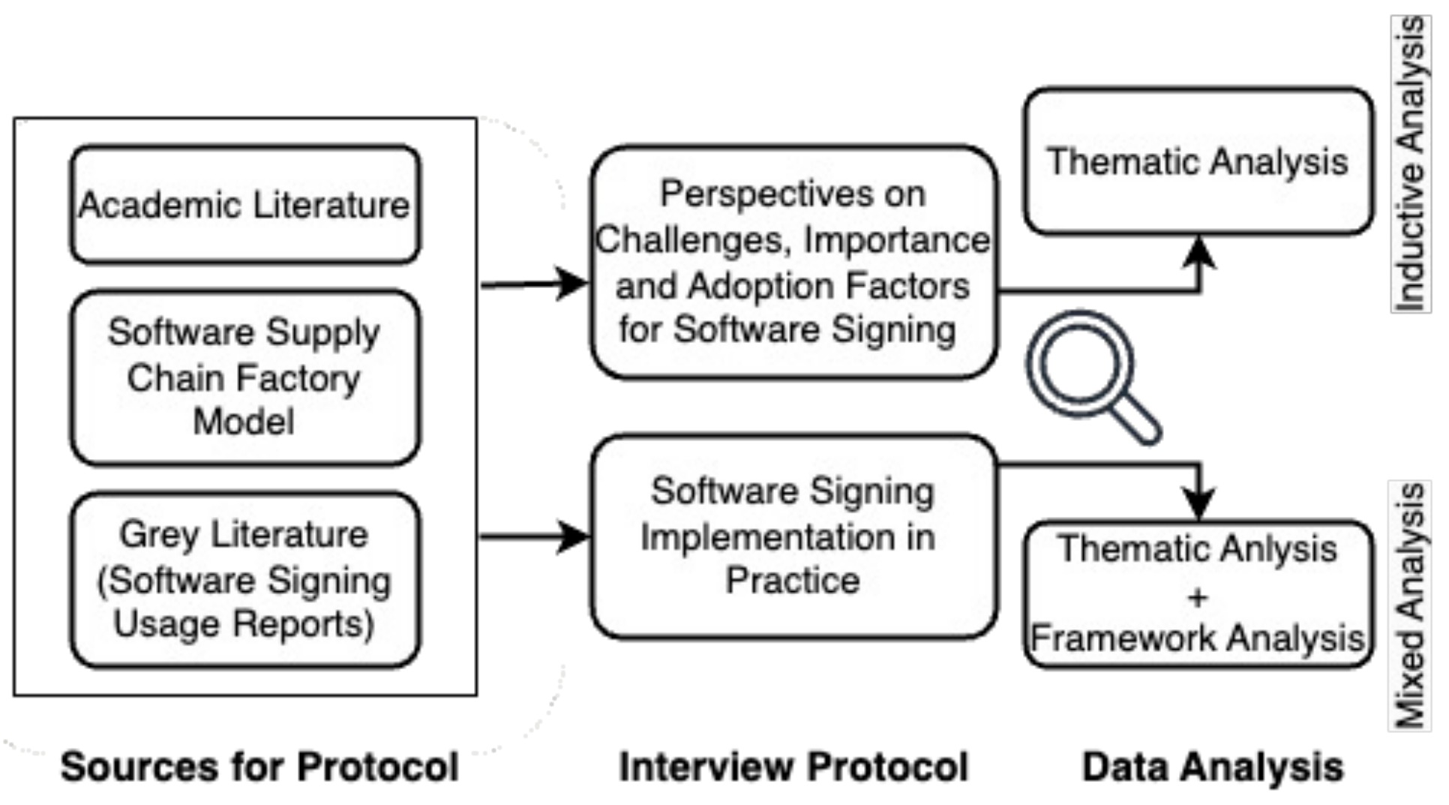
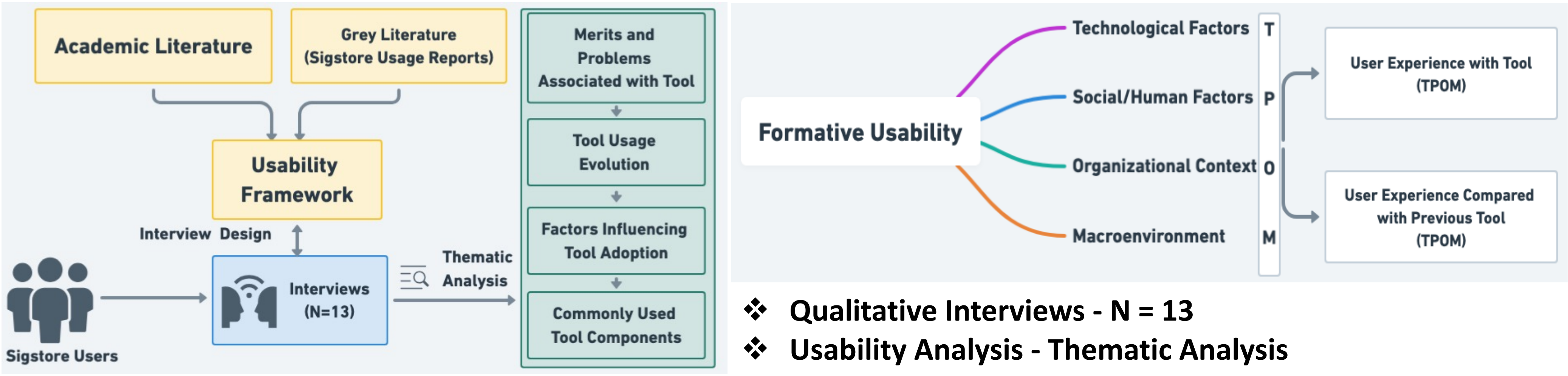

Academic Literature
Software Supply Chain Factory Model
Grey Literature (Software Signing Usage Reports)
Perspectives on Challenges, Importance and Adoption Factors for Software Signing
Software Signing Implementation in Practice
Thematic Analysis
Inductive Analysis
Thematic Anlysis + Framework Analysis
Mixed Analysis
Sources for Protocol
Interview Protocol
Data Analysis

Figure 3. Methodology to study industrial practices of software signing


Academic Literature
Grey Literature (Sigstore Usage Reports)
Usability Framework
Interview Design
Sigstore Users
Interviews (N=13)
Thematic Analysis
Merits and Problems Associated with Tool
Tool Usage Evolution
Factors Influencing Tool Adoption
Commonly Used Tool Components
Formative Usability
Technological Factors
Social/Human Factors
Organizational Context
Macroenvironment
T
P
O
M
User Experience with Tool (TPOM)
User Experience Compared with Previous Tool (TPOM)

- ❖ Qualitative Interviews - N = 13
- ❖ Usability Analysis - Thematic Analysis

Figure 4. Methodology to study the usability of software signing tools

Refined Supply Chain Factory Model

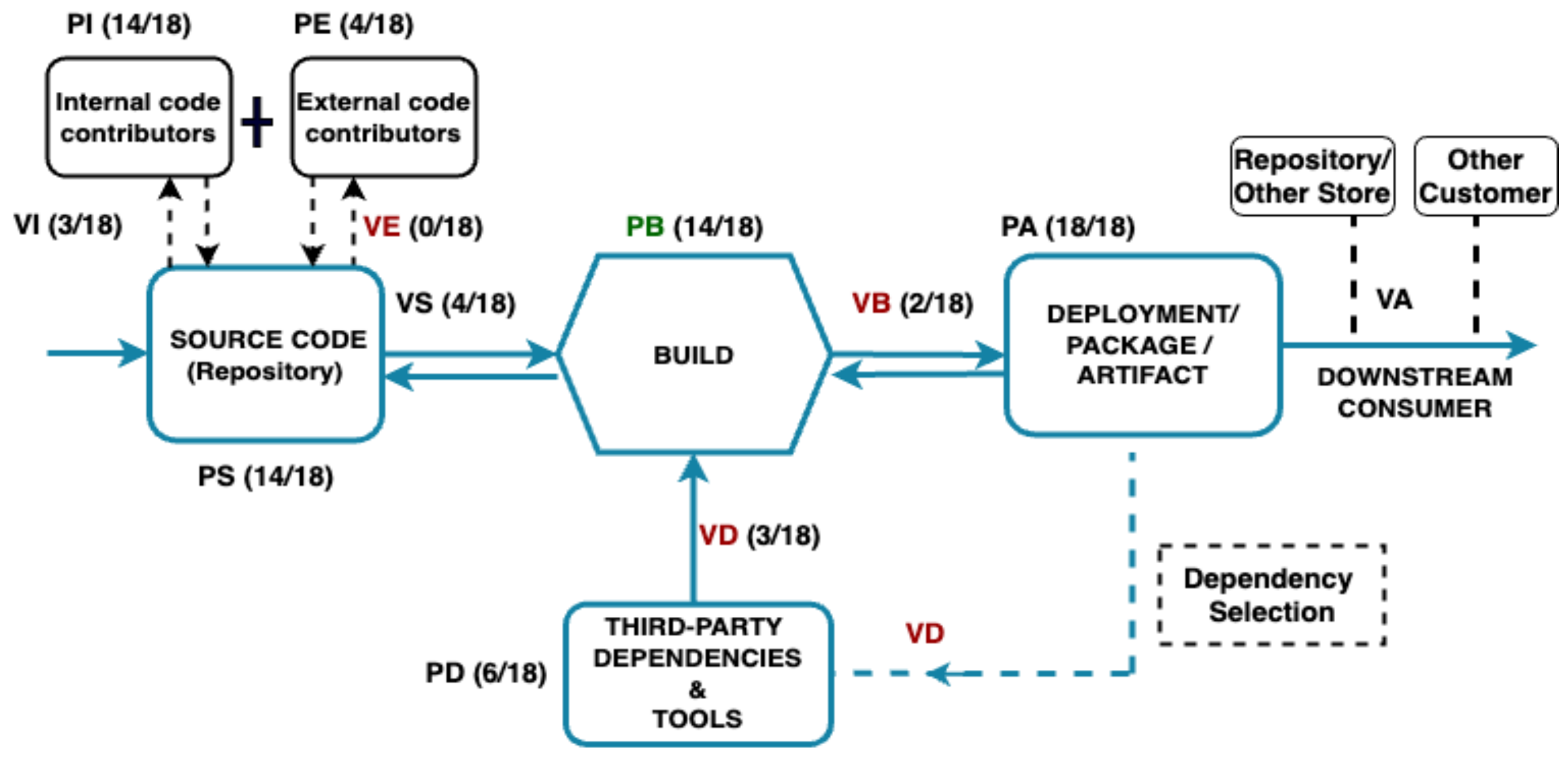


Figure 5. Our refined software supply chain factory model highlighting different points where software Signing is used in practice and how many practitioners who did use them.

Challenges Affecting Software Signing Implementation in Practice.

Observed Challenges	#Subjects	#Orgs	Subjects' Proposed Solutions
Technical			
Key Management	10	9	Use of Keyless Signing (*e.g.,* Sigstore)
Compatibility Issues	6	6	—
Lack of Verification of Signatures	6	5	Signed Metadata, Component Data Management
Ease of Use/Usability	4	4	Usable Signing Tools (*e.g.,* Sigstore), Documentation
No Unifying Standard	2	2	—
Organizational			
Operationalization of the Signing Process	4	4	Automating Signing
Resources to Set up Signing	3	3	—
Creating Effective Signing Policy	2	2	Regular Process Feedback Mechanisms
No Management Incentive to Sign	2	2	—
Bureaucracy	1	1	—
Human			
Expertise in setting setup and use of signing	5	4	—
Developer Attitude to Signing	3	3	Automating Signing
Lack of Demand from Customers	1	1	—

Figure 6. Challenges to software signing implementation in practice. We categorize related challenges into – ***Technical***, ***Organizational***, and ***Human*** challenges.

Problems & Strengths of Software Signing Tool (Sigstore)

Strength

Topics & Associated Examples	Subjects
Technological Factors	
Ease of Use	**8**
Signing Workflow & Verification	P1, P2, P7, P8, P10-13
Setting up with automated CI/CD actions	P9
No key distribution problems	P1
Use of Short-lived Keys & Certificate	**3** –P2, P3, P11
Signer ID Management	**4**
Use of OIDC(Keyless) to authenticate signers	P3, P5, P10, P12
Compatibility with Several New Technologies	**4**
Integrability with SLSA build	P12
Integrability with several container registries/technologies	P9, P10
Integrability with several cloud-native applications	P11
Precence of a Transparency Log	**3**
Transparency logs increase security	P5, P10
Evaluation of signing adoption using logs	P8
Bundling Signatures With Provenance Attestations	**2** – P3, P4
Reliability of Service	**1** – P7
Macroenvironmental Factors	
Free/Open-Source	**2** – P7, P13

Problems

Topics & Associated Examples	Subjects
Enterprise Adoption Limitations	**7**
Rate Limiting Problems – ***T***	P3, P7, P10, P11
Lack of dedicated Support & Maintenance – ***T & P***	P11, P2
Not Suited for Regulated Organizations – ***M & O***	P3
Latency Concerns – ***T***	P6
Transparency Log Issues	**6**
Not Suitable for private Setup – ***T***	P2, P3, P6, P10, P13
Use in Air Gap Conditions – ***T***	P2, P3, P8
Efforts to Monitor Logs – ***P***	P2
Private Sigstore Instance Setup	**5**
Documentation – ***P***	P8, P9, P6
Limited Community Support – ***M***	P11
Infrastructure Requirements & Maintenance Costs – ***T***	P5, P6
Other Documentations and Usage Information Issues – ***P***	**3** — P1, P10, P13
Integration to Other Systems	**3**
Attestation Storage – ***T***	P1
Gitlab & Jenkins – ***T***	P8
Other Unsupported technologies – ***T***	P12
Offline Capabilities – ***T***	**2** – P3, P4
Fulcio Issues	**1** – P3
Timestamping Issues – ***T***	
Fulcio-OIDC Workflow – ***T***	
Software Libraries – ***T***	**1** – P7

Figure 5. Practitioner-Reported Advantages of Sigstore and difficulties in using Sigstore. We indicate the associated usability factor of each category of weakness using **– T-technology, P- social/human, O-organizational, M-macroenvironmental factors.**

Why Practitioners Switch Software Signing Tools

Topics & Associated Examples	Subjects
Human/Social Factors	
Practitioners Contribute to Sigstore	6 – P2, P4, P6, P7, P8, P10
GPG Issues	6
Low adoption rates	P1, P10
Key management issues & Other usability concerns	P1, P6, P9, P12, P13
Steep learning curve	P9, P12
Compatibility with newer technology	P12
Notary Issues	2
Non-demand from customers	P9
Compatibility with other tools	P9
Lack of regular updates	P9
Key & Identity Management	P5
Proprietary Tool Issues	1
Difficult to setup	P11
Technological Factors	
Available Sigstore Functionalities	3 – P1, P5, P10
A transparency log, etc	P5, P10
Compatibility to other Tools	P1
Macroenvironmental Factors	
Regulation & Standards	4 – P5, P6, P11, P13
Large User Community	1 – P8
Inherent Trust of Creators	1
Trust of CNCF products	P3

Figure 7. Reasons Practitioners Choose or Switch to Sigstore Before Adoption.

Future Work

1. Establishing trust metrics in open source with software signatures.
2. Signature verification in the software engineering process .
3. Cross-ecosystem software signature interchange.

References

1. Schorlemmer, Taylor R., et al. "Signing in four public software package registries: Quantity, quality, and influencing factors." IEEE Symposium on Security and Privacy (SP). IEEE, 2024.

PURDUE UNIVERSITY