Bezpečnost vývoje a code signing

Pro zajištění důvěryhodnosti dodavatelského řetězce

12.4.2023

AFCEA – BS69 – Bezpečnostní seminář:
Bezpečnost dodavatelských řetězců & Digitální transformace státu

Dalibor Premus

3KEYCOMPANY

NIS2

Opatření k řízení kybernetických bezpečnostních rizik

a) politiku analýzy rizik a politiku bezpečnosti informačních systémů;

b) řešení incidentů;

c) řízení kontinuity provozu, jako je například správa zálohování a obnova provozu po havárii, a krizové řízení;

d) bezpečnost dodavatelského řetězce včetně bezpečnostních aspektů týkajících se vztahů mezi každým subjektem a jeho přímými dodavateli nebo poskytovateli služeb;

e) zabezpečení pořizování, vývoje a údržby sítí a informačních systémů, včetně zveřejňování zranitelností a jejich řešení;

f) politiky a postupy za účelem posouzení účinnosti opatření k řízení kybernetických bezpečnostních rizik;

g) základní postupy kybernetické hygieny a školení v oblasti kybernetické bezpečnosti;

h) politiky a postupy týkající se používání kryptografie a případně šifrování;

i) bezpečnost lidských zdrojů, postupy kontroly přístupu a správa aktiv;

j) v příslušných případech používání vícefaktorových autentizačních řešení nebo trvalých autentizačních řešení, zabezpečené hlasové, obrazové a textové komunikace a zabezpečených systémů nouzové komunikace v rámci subjektu.

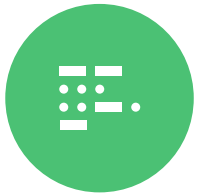
BEZPEČNÝ SW VÝVOJ

Principy bezpečného vývoje

Modelování hrozeb

Analýza bezpečnostních rizik

Design



Řízení zdrojových kódů

Kontrola kódu

Školení

BEZPEČNÝ SW VÝVOJ

Procesy, směrnice, postupy

Verzování	Metodika verzování, která je aplikována na vývoj softwaru a jeho komponent, společně s postupem, jak řídit výjimky
Architektura a design	Požadavky na architekturu a design vyvíjeného softwaru a jeho komponent. Obsahuje požadavky na modelování aplikačních hrozeb a řízení souvisejících rizik
Data a soukromí	Požadavky a postupy pro ochranu osobních a citlivých dat v softwaru a během tranzitu informací mezi komponenty
Šifrování	Požadavky na práci s kryptografickými klíči a šiframi, které obsahují povolené algoritmy, řízení životního cyklus a identit
Řízení přístupu	Požadavky spojené s autentizací uživatelů a systémů a přístupová pravidla a oprávnění
Integrace	Jakým způsobem je řízena bezpečná integrace třetích stran se seftwarem
Kvalita kódu	Požadavky a postupy pro měření kvality kódu při vývoji softwaru
Vydávání	Proces vydávání verzí, souhrn provedených změn v softwaru, bezpečná aktualizace, integritu vydávaného kódu a softwaru
Odolnost	Požadavky na schopnost softwaru reagovat na bezpečnostní incidenty
Kontrola kódu	Požadavky na to, jak provádět kontroly kódu softwaru

Supply chain attacks are not common and the SolarWinds Supply-Chain Attack is one of the most potentially damaging attacks we've seen in recent memory. Of course, as it is an evolving situation, we will likely know more as the days progress, but this is what we know as of now.

On December 8 FireEye announced that it had been hacked by a nation-state and since that announcement they've been incredibly transparent, publishing information about the breach and what they've learned about it in their investigation.

SolarWinds Breach

On December 13 Chris Bing of Reuters broke the story that the US Treasury Department has been compromised by a sophisticated adversary. Shortly after, Ellen Nakashima of the Washington Post confirmed with background sources that the US Treasury breach was perpetrated by the same group that targeted FireEye, that SolarWinds was involved in both breaches, and that it was perpetrated by threat group APT29 (Cozy Bear/Russian SVR).

SUPPLY CHAIN BEZPEČNOST

- Sunburst backdoor vložen do kódu během vývoje produktu
- Software update proces kompromitován
- Nepodepsaný kód vývojářů
- Napadeno více než 18.000 zákazníků včetně vládních organizací
- Obrovský finanční a reputační dopad

Stolen Nvidia certificates used to sign malware—here's what to do

Posted: March 15, 2022 by Pieter Arntz

Nvidia, the ransomware breach with some plot twists

Posted: March 3, 2022 by Pieter Arntz

On February 25, news broke about a cyberattack on Nvidia, America's biggest microchip company, which saw parts of its business taken offline for two days. Soon after, the ransomware group LAPSUS$ claimed responsibility and threatened to leak 1 TB in exfiltrated data.

You would think that while this is big news, the story is one that has been told many times. So many times that ransomware fatigue is starting to become the new security fatigue. But there are some interesting aspects to this particular attack that make it stand out.

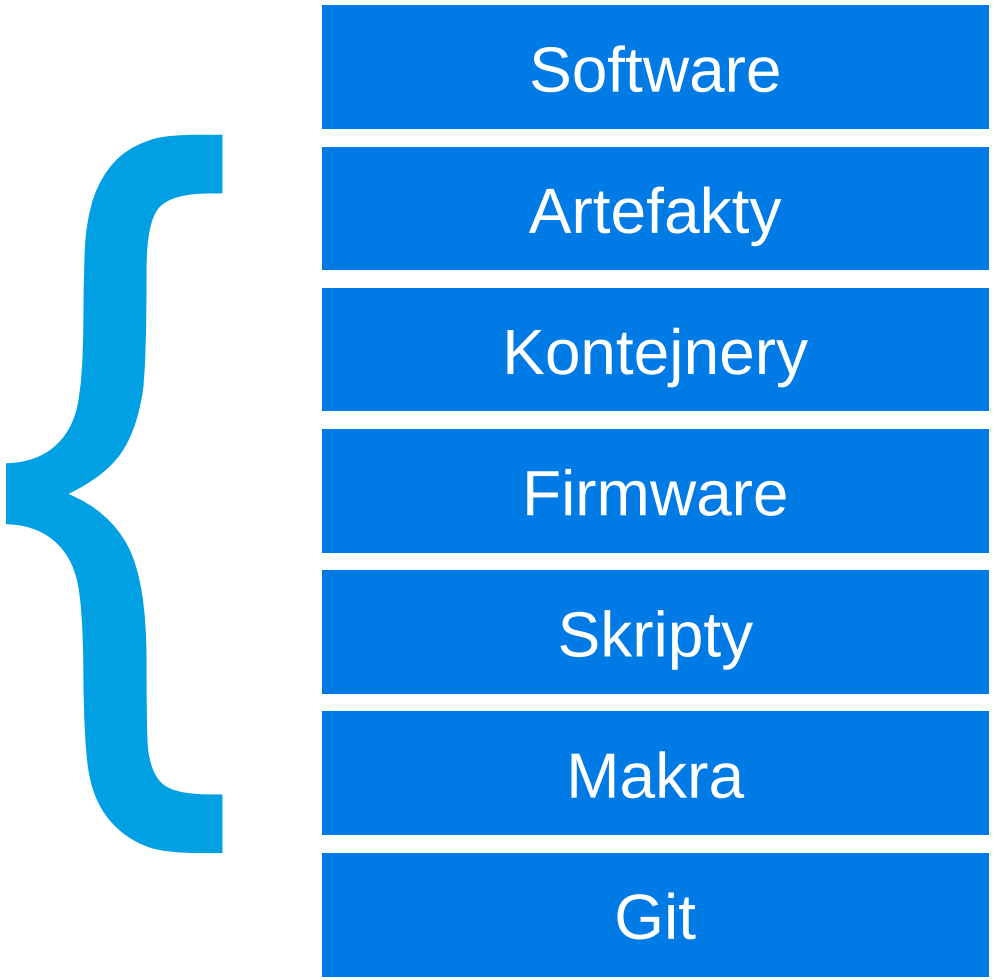
trusted sources. This is a powerful security feature, provided that code signing certificates are kept out of the hands of cybercriminals.

KOMPROMITACE IDENTITY

- Odcizené code-signing certifikáty včetně privátních klíčů (exspirované)
- Možnosti instalace driverů podepsaných exspirovaným certifikátem

CODE SIGNING

- Podepisování kódu je proces digitálního podepisování dat potvrzení autora softwaru a zaručení, že kód nebyl od podepsání změněn.
- Definice „kódu“ se mění. S příchodem moderních technologií a postupů, jako je jsou například softwarově definovaná infrastruktura, nebo agilní DevOps přístup, podepisujeme nejen softwarový kód.
- Prakticky každá společnost podepisuje kód v nějaké podobě nebo formě.
- Podepisování kódu je součástí bezpečného vývoje softwaru. Automatizace pomáhá pro zvýšení logické bezpečnosti.

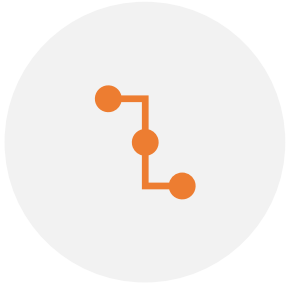


CODE SIGNING

Potenciální hrozby

Kryptografické klíče

Kompromitace klíčů z nezabezpečeného systému



Aktualizace kódu

Neoprávněné nebo nedetekované vložení kódu

Kompromitace systému

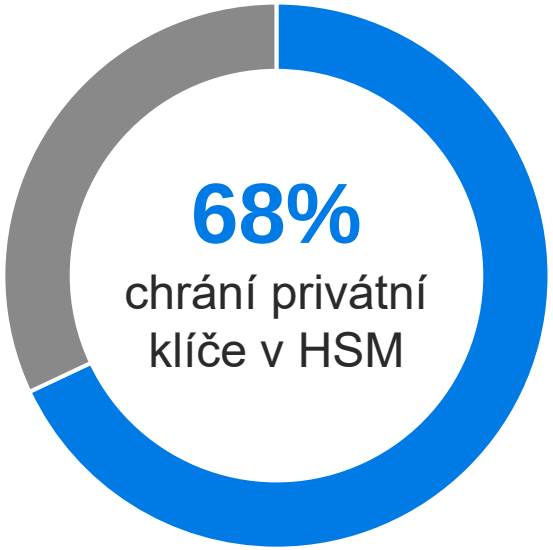
Neautorizovaný přístup k build serverům

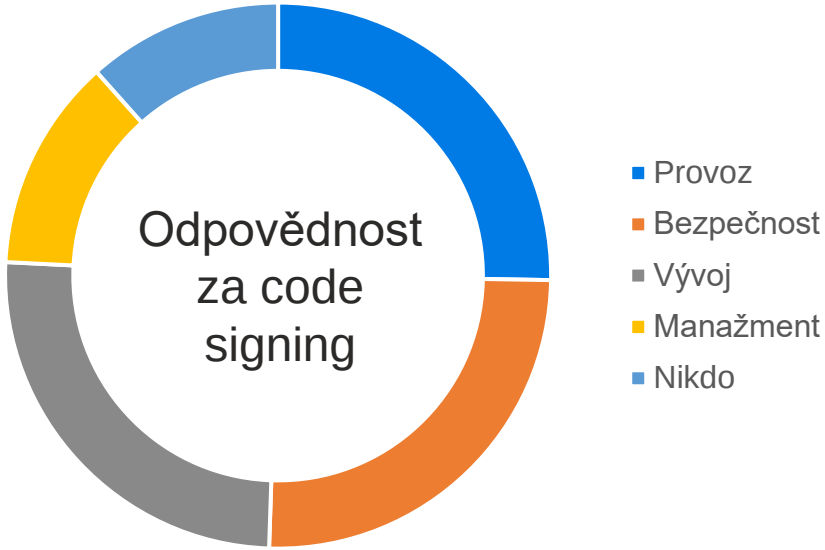
Vnitřní hrozba

Záměrné nebo neúmyslné zveřejnění kódů a klíčů

CODE SIGNING

Statistiky

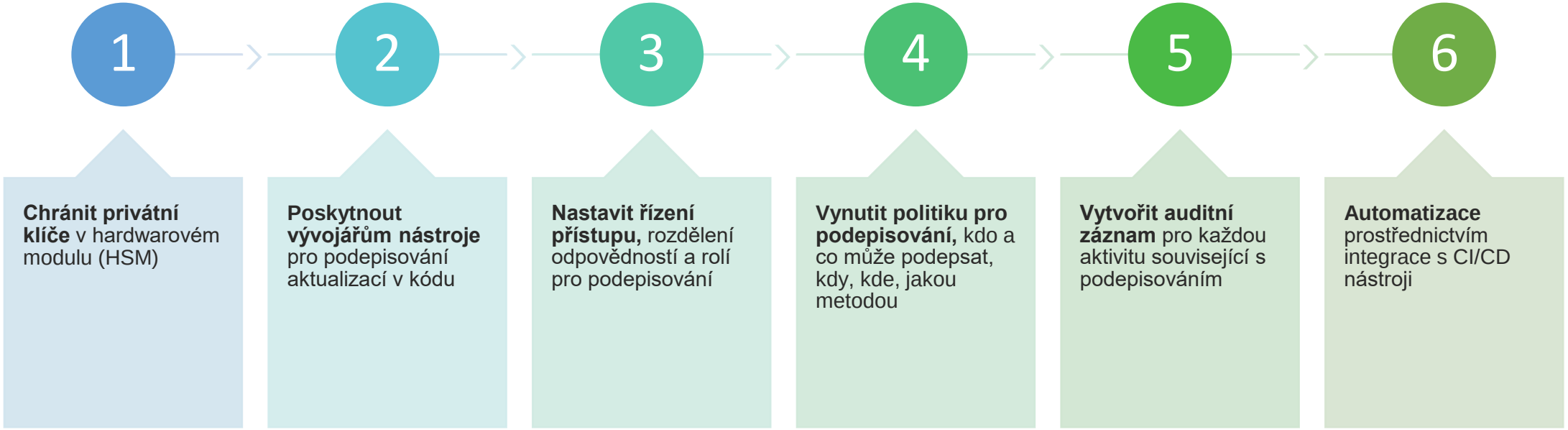




* State of Machine Identity Management 2023

CODE SIGNING

Na co myslet

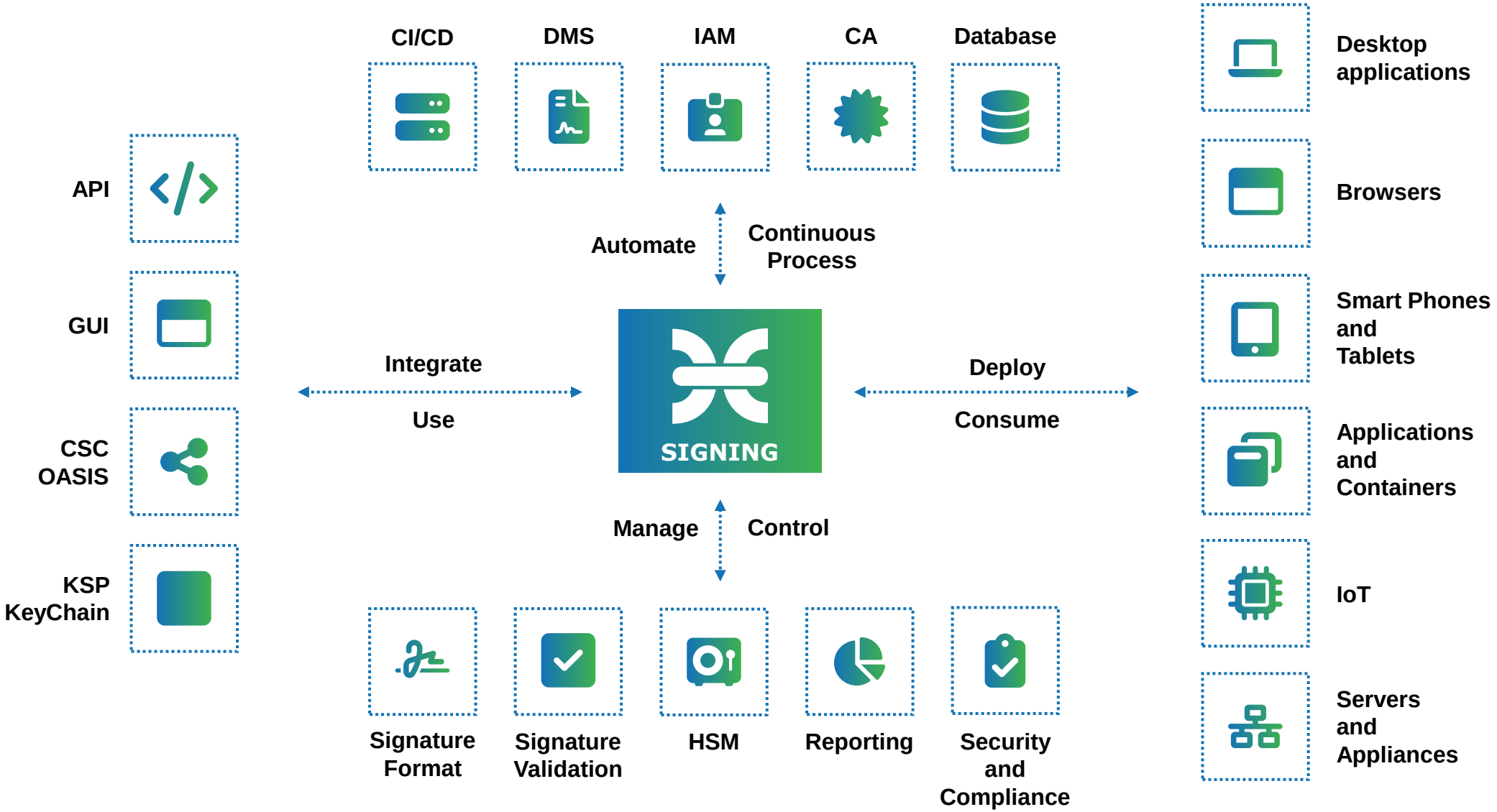


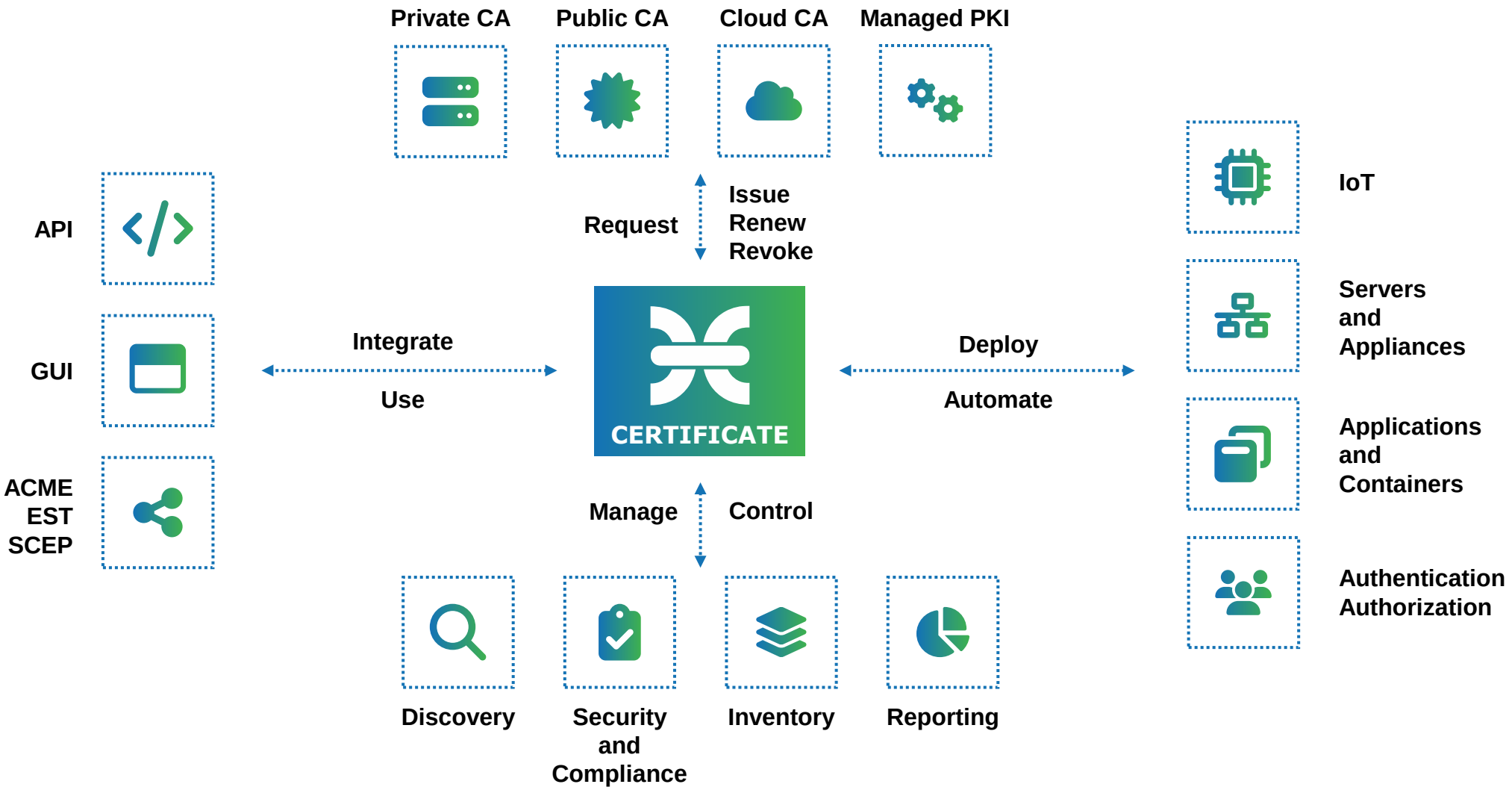
OPEN SOURCE

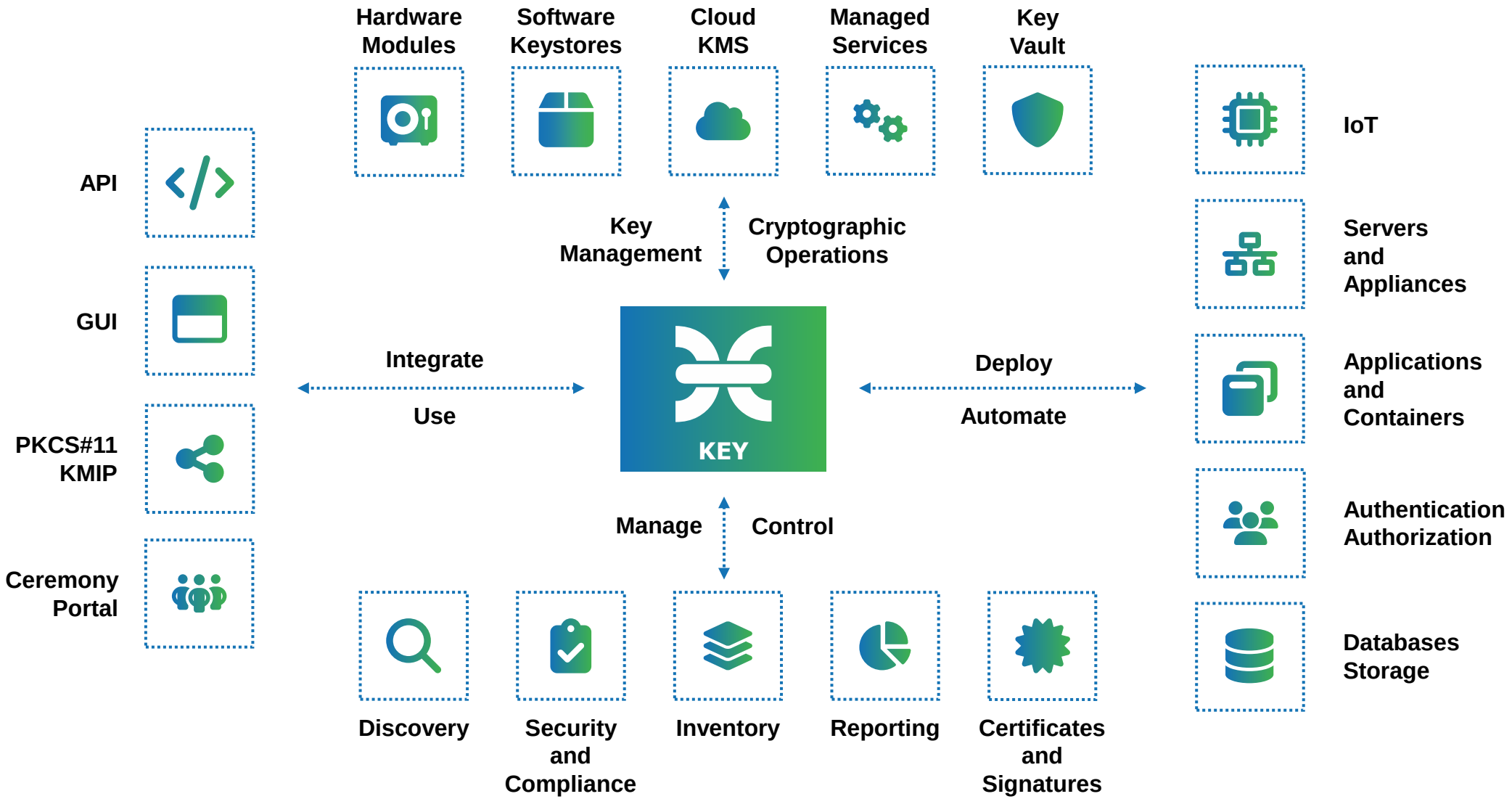
NIS2 směrnice:

*„**Nástroje a aplikace kybernetické bezpečnosti s otevřeným zdrojovým kódem mohou přispívat k vyšší míře otevřenosti a mohou mít pozitivní dopad na účinnost průmyslové inovace.** Otevřené normy usnadňují interoperabilitu mezi bezpečnostními nástroji a přispívají k bezpečnosti odvětvových zúčastněných stran. Nástroje a aplikace kybernetické bezpečnosti s otevřeným zdrojovým kódem mohou podpořit širší komunitu vývojářů, a umožnit tak diverzifikaci dodavatelů. **Otevřený zdrojový kód může vést k větší transparentnosti při ověřování nástrojů souvisejících s kybernetickou bezpečností a k postupu odhalování zranitelností řízeném komunitou.** Členské státy by proto měly mít možnost podporovat používání softwaru s otevřeným zdrojovým kódem a otevřených standardů tím, že budou provádět politiky spojené s využíváním otevřených dat a otevřených zdrojů v rámci koncepce „bezpečnost prostřednictvím transparentnosti“. Politiky, které podporují zavádění a udržitelné využívání nástrojů kybernetické bezpečnosti s otevřeným zdrojovým kódem, **mají zvláštní význam pro malé a střední podniky, které se potýkají se značnými realizačními náklady, jež by bylo možné minimalizovat snížením potřeby specifických aplikací nebo nástrojů.**“*


CZERTAINLY
/ˈsɜːrtnli/
Follow us on:







3KEYCOMPANY

3Key Company s.r.o.

Dalibor Premus

dalibor.premus@3key.company