

Stručný obsah

1. Symetrická a asymetrická kryptografie	21
2. Prostředky pro bezpečné ukládání aktiv	37
3. Certifikáty a certifikační autority	53
4. Žádost o certifikát	79
5. Odvolávání certifikátu	87
6. Certifikační cesta a důvěryhodné kotvy	95
7. Ověřování platnosti certifikátu a poznámka k ověřování digitálního podpisu	107
8. Obnovování certifikátů	115
9. PKI nejsou jen certifikáty	121
10. Kvalifikované certifikáty a zaručené podpisy	125
11. Má první certifikační autorita	139
12. Ethereum	157
13. ASN.1, BER, DER, UTF-8 a Base64	169
14. Žádost o vydání certifikátu pod lupou	195
15. Certifikát pod lupou	205
16. Odvolání certifikátu pod lupou	253
17. CMP a CMC	271
18. Budujeme certifikační autoritu	293
19. Atributové certifikáty	317
20. Časová razítka	339
21. E-notary	363
22. Protokol TLS	373
23. PKCS#7 a CMS	407
24. Bezpečná pošta	433
25. Dlouhodobý digitální podpis	479
26. Dlouhodobá archivace nejenom digitálně podepsaných dokumentů	503
27. Budujeme PKI, TSA a důvěryhodné archivy	515