

Obsah

Zoznam skratiek	7
Zoznam vybraných pojmov	11
Zoznam obrázkov	13
Úvod	15
1. Prvky a technológie pre riadenie prístupu	17
1.1. Autentifikačný server	17
1.2. Server politiky.....	17
1.3. Server pre prístup k sieti	17
1.4. Kerberos	18
1.5. RADIUS	19
1.6. Adresárová služba.....	21
1.7. Ďalšie technológie.....	23
1.7.1. OpenID (OpenID Connect)	23
1.7.2. SAML (Security Assertion Markup Language)	23
1.7.3. ALFA (XACML).....	25
2. Overovacie prvky	31
2.1. Token	31
2.2. Bezpečnostný token	31
2.3. Hardvérový kľúč.....	34
2.4. Autentifikátor	36
2.5. Ďalšie možnosti.....	36
3. Biometria	39
3.1. Základné pojmy	40
3.2. Charakteristiky biometrickej autentifikácie	44
3.3. Princíp činnosti biometrických systémov	45
3.4. Základné biometrické technológie	47
3.4.1. Rozpoznávanie ruky, prstov a písma	47
3.4.1.1. Rozpoznávanie odtlačku prsta (Fingerprint Recognition)	47
3.4.1.2. Spracovávanie a porovnávanie odtlačkov.....	51
3.4.1.3. Geometria ruky	54
3.4.1.4. Odtlačok dlane	56
3.4.1.5. Krvné riečisko ruky	57
3.4.1.6. Lôžko nechty	58
3.4.2. Písmo a podpis	59
3.4.2.1. Dynamika podpisu.....	59
3.4.2.2. Rozpoznávanie podpisu	60
3.4.2.3. Písanie na klávesnici	61
3.4.2.4. Analýza písania.....	62
3.4.2.5. Analýza podpisu	63
3.4.2.6. Analýza pohybu myši.....	63
3.4.3. Rozpoznávanie podľa očí.....	64
3.4.3.1. Rozpoznávanie dúhovky.....	64
3.4.3.2. Identifikácia pomocou očnej sietnice	67
3.4.4. Rozpoznávanie tváre	68
3.4.4.1. Metódy rozpoznávania tváre	69
3.4.4.2. Geometria tváre.....	71
3.4.4.3. Metóda porovnávania obrazov	73
3.4.4.4. Lokalizácia hlavy.....	75
3.4.4.5. 3D verifikácia tváre	76

3.4.4.6. 3D rozpoznávanie tváre	77
3.4.5. Termografia - infračervené zobrazovanie	78
3.4.6. Rozpoznávanie hlasu (Voice Recognition).....	81
3.4.6.1. Overovanie hlasu	81
3.4.6.2. Textovo závislé systémy	82
3.4.7. Neštandardné biotechnológie	83
3.4.7.1. Biometria ucha	83
3.4.7.2. DNA	84
3.4.7.3. Kinematika a dynamika ľudskej chôdze	85
3.4.7.4. Multimodálne biometrické riešenia	89
3.4.8. Ostatné biometrické technológie	91
4. Prístup a informačné technológie	93
4.1. Prístup k médiu	93
4.1.1. CSMA	94
4.1.2. CSMA/CD	95
4.1.3. CSMA/CA	96
4.2. Riadenie prístupu do siete	98
4.2.1. Prístup do cloudu	101
4.2.2. CAN bus	101
4.3. Technológie RFID v riadení prístupu	105
4.3.1. Elektronické sledovanie tovaru	107
4.3.1.1. Rádiofrekvenčné systémy	109
4.3.1.2. Mikrovlnné systémy	111
4.3.1.3. Systémy s frekvenčným delením	114
4.3.1.4. Elektromagnetické systémy	114
4.3.1.5. Akusticko-magnetický systém	117
4.3.2. Karty pre systémy riadenia prístupu	120
5. Digitálna identita	125
5.1. Online identita	125
5.1.1. Sieťová identita	128
5.1.2. Sebestačná identita	129
5.2. Digitálny identifikátor	130
5.2.1. Handle System	131
5.2.2. Taxonómia identity	132
5.3. Elektronická autentifikácia	132
5.4. eIDAS	134
5.4.1. Obsah certifikátu	135
5.4.2. Revokačné systémy	137
5.4.3. Špecifické druhy certifikátov	138
5.4.4. Typy kvalifikovaných certifikátov	139
6. Šifrovanie a kódovanie	141
6.1. História kryptografie	141
6.1.1. Klasická kryptografia	142
6.1.1.1. Cézarova šifra	143
6.1.1.2. Skytalé	144
6.1.2. Stredoveká kryptografia	145
6.1.2.1. Jednoduchá stĺpcová transpozícia	146
6.1.2.2. Vigenierova šifra	147
6.1.3. Kryptografie od roku 1800 do druhej svetovej vojny	150
6.1.4. Substitučná šifra	152

6.1.5. Šifrovacie systémy vo vojenskej komunikácii	154
6.1.6. Steganografia	157
6.1.6.1. Neviditeľné atramenty	158
6.1.6.2. Digitálna steganografia	158
6.2. Moderné šifry	159
6.2.1. Symetrické šifrovanie	159
6.2.2. Asymetrické šifrovanie	160
6.2.3. Hashovacie funkcie.....	163
6.2.3.1. Jednocestná funkcia	164
6.2.3.2. Jednocestná funkcia so zadnými dvierkami	164
6.2.4. Ostatné druhy šifrovania	165
6.3. Elektronický podpis	166
6.3.1. Certifikačná autorita	169
6.3.2. Dôveryhodná tretia strana a siete dôvery.....	170
6.3.3. Časová pečiatka	171
Záver	173
Použité zdroje	175
Prílohy	177
A. Lúštenie šifry pomocou frekvenčnej analýzy.....	177
B. Pôvod názvu Kerberos	179