



Security and Privacy Challenges with Biometric Solutions

Koen Simoens
K.U.Leuven – COSIC

LSEC Biometrics 2011, Leuven

Outline

- Biometric system security in 5 slides
- Motivating biometric template protection
- Some remarks
- Examples and standardization
- Evaluating template protection

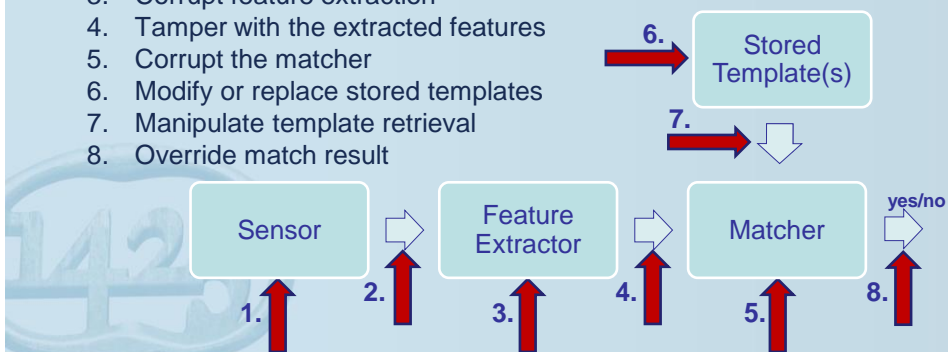


Biometric System Security

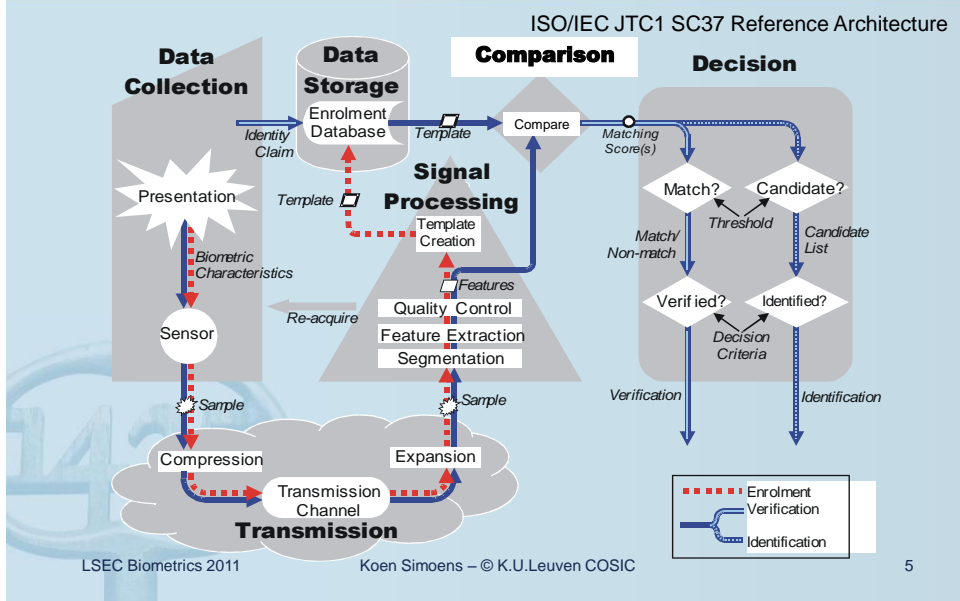
Attack Points – How to get in?

Ratha, Connell, & Bolle. 2001. *Enhancing Security and Privacy in Biometrics-Based Authentication Systems*

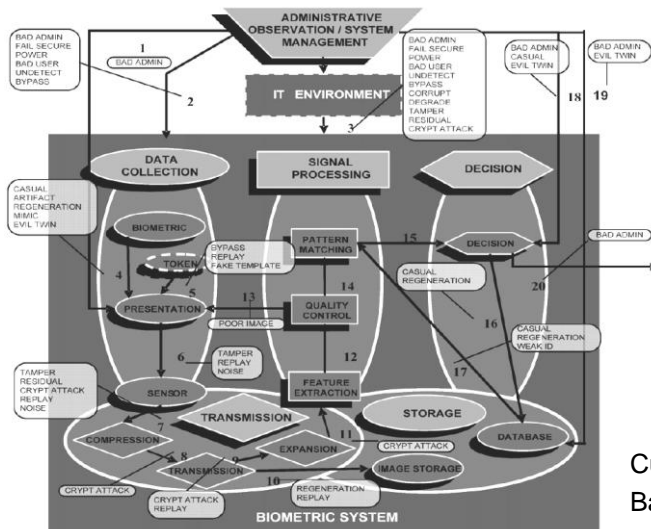
1. Present fake biometrics to the sensor;
2. Replay attack and sensor bypass;
3. Corrupt feature extraction
4. Tamper with the extracted features
5. Corrupt the matcher
6. Modify or replace stored templates
7. Manipulate template retrieval
8. Override match result



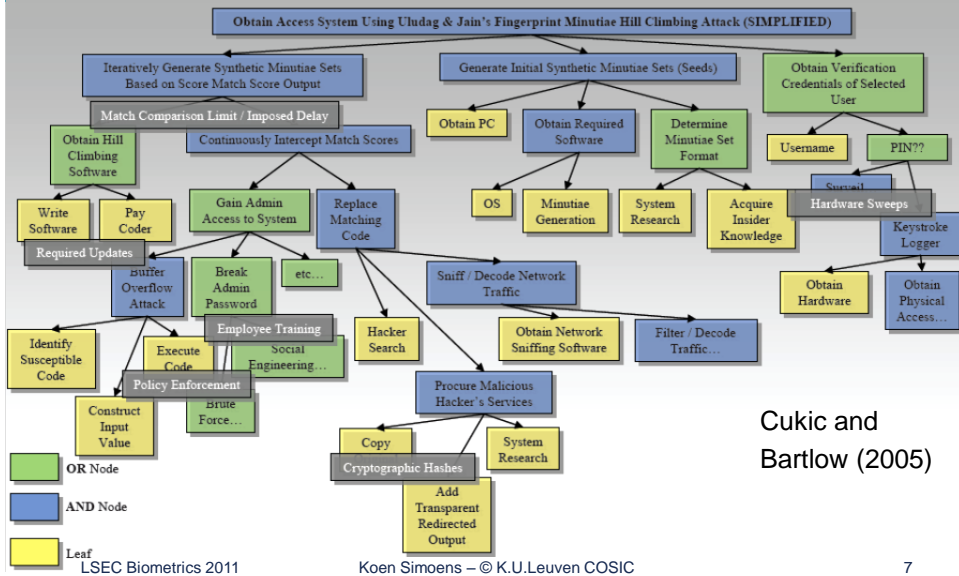
Biometric Reference Architecture



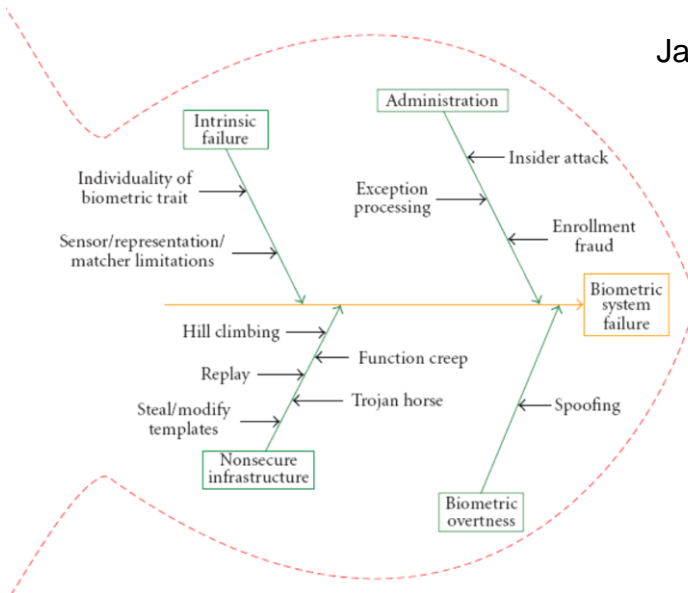
More Threats and Attack Points



Risk Management and Attack Trees



Categorization of Vulnerabilities



Common Criteria – Certification

- BSI (Bundesamt für Sicherheit in der Informationstechnik). (2008). *Biometric Verification Mechanisms Protection Profile Version 1.3*.
– <http://www.commoncriteriaportal.org/files/ppfiles/pp0043b.pdf>
- IAD (Information Assurance Directorate). (2007, Version 1.1). *U.S. Government Biometric Verification Mode Protection Profile for Basic Robustness Environments*.
– http://www.commoncriteriaportal.org/files/ppfiles/pp_bvm_br_v1.1.pdf
- IAD (Information Assurance Directorate). (2007, Version 1.1). *U.S. Government Biometric Verification Mode Protection Profile for Medium Robustness Environments*.
– http://www.commoncriteriaportal.org/files/ppfiles/pp_bvm_mr_v1.1.pdf



Motivating Biometric Template Protection

Observations

- *EU aims to stop 'visa shopping' : Schengen states to share visa data (2007-06-08)*
 - In the EU, **supervised access** to the biometric databases of the European Visa Information System (VIS) is granted to policy and Europol.
 - http://www.theregister.co.uk/2007/06/08/schengen visa_data/
- *India to issue all 1.2 billion citizens with biometric ID cards (2009-07-15)*
 - Mr Nilekani, who left ... to take up his new job, wants the cards to be linked to a **"ubiquitous online database"** accessible from anywhere.
 - <http://www.telegraph.co.uk/news/worldnews/asia/india/5831929/India-to-issue-all-1.2-billion-citizens-with-biometric-ID-cards.html>
- *DHS develops shared biometrics database with DOD (2011-03-08)*
 - In the USA, the Department of Homeland Security (DHS) is developing a joint database with the Department of Defence (DOD) **for the purpose of accessing current biometric data stored by DOD.**
 - <http://homelandsecuritynewswire.com/dhs-develops-shared-biometrics-database-dod>
- **Biometrics data increasingly shared**

Observations

- Biometrics are a success
 - Forensics, immigration services, access control
 - Convenient and reliable
- Security and privacy issues with biometric templates
 - **Impersonation**
 - If you can read a password, you can use it
 - Reference template allows constructing artificial prints
 - **Sensitivity**
 - Biometrics may contain sensitive information
 - **Linkability**
 - Templates are unique identifiers => cross-matching
 - Other
 - Substitution attacks, DoS, ...
 - Prabhakar et al. (2003). Biometric recognitions: security and privacy concerns
- **Conclusion: do not store reference data in the clear**

Observations



- Biometrics are no longer in your pocket
- At the same time, increased awareness of privacy
 - Security and privacy issues stemming from the use of biometrics
 - PETFs, data protection authorities, Privacy-by-Design, ...
- **Increasing but conflicting demands** (growing gap)

Protecting Biometric Data

- **Biometric template protection** to bridge the gap
 - Template-level protection
 - Fuzzy commitment, fuzzy vault, cancellable biometrics,...
 - System-level protection
 - Physical security, procedures, encryption, hardware-based/-assisted (smartcards, TPM)
 - Protocol-level
 - Advanced protocols relying on crypto primitives (MPC, homomorphic encryption, PIR)
- Main challenges:
 - Hide biometric data (**irreversibility**)
 - Prevent cross-matching of hidden data (**unlinkability**)
 - **Maintain performance/accuracy** without giving up functionality

On the Concepts Security and Privacy

- Stop using them without explaining what you mean!
- Distinguish between
 - Primary assets
 - What are you protecting with your biometric system?
 - Secondary assets
 - Biometric data/templates (scope of template protection)
- Security and privacy of templates
 - Be more specific: irreversibility and unlinkability
 - Distinguish information-level aspect and system aspects
 - Attack scenarios

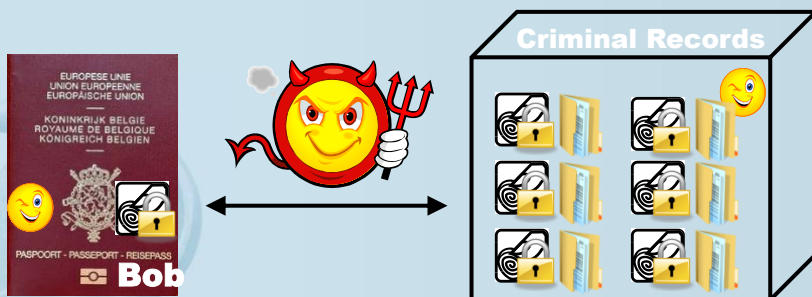
Attack Scenario: Deanonimization

- Bob has access to high-level security zones in his company
- Attacker
 - Has Bob's passport with protected fingerprint
 - Has employee (access) card with protected fingerprint
 - Wants to know if it's Bob's
 - Does not give immediate access but worth investigating



Attack Scenario: Database Lookup

- Attacker
 - Has Bob's passport with protected fingerprint
 - Has access to database of **anonymized** criminal **records** and protected fingerprints
 - Knows bob is in there and wants to find his record



LSEC Biometrics 2011

Koen Simoens – © K.U.Leuven COSIC

17

Attack Scenario: Reversing

- Solution for dealing with linkability:
 - Create incompatible templates
- Equivalent to using **different schemes in different applications**
 - Same principles, different error-correcting codes
- Both leak **(different)** information: can this be combined?
 - Assume that attacker knows templates are related



LSEC Bio

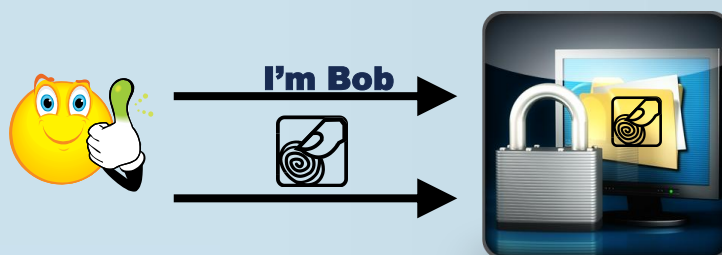
Koen Simoens – © K.U.Leuven COSIC

18



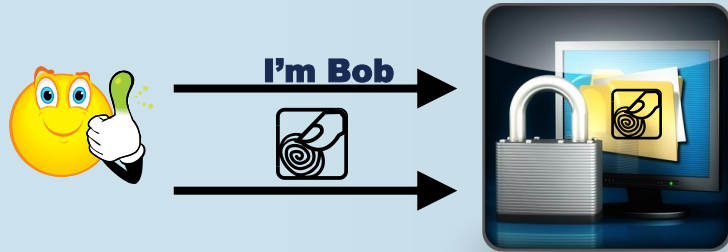
Some Remarks

Biometric Authentication



- Bob claims and proves identity towards system
- Verification: **compare proof against reference**
- Two prints of same finger never exactly the same
 - Verification is **similarity check** (as opposed to passwords)

Biometric Authentication



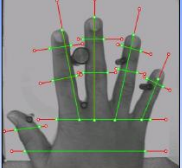


- Bob claims and proves identity towards system
- Verification: **compare proof against reference**
- Two prints of same finger never exactly the same
 - Verification is **similarity check** (as opposed to exact match)

Password hashing does not work

Example Data Representations

Fixed-length vector	Fixed-length vector	Variable-length 3-tuple	Binary string
<p>[65 53 59 52 62 4747 45 255 333 253 287 243 149]</p>	<p>[-315.91, -441.10, 212.35, -90.78, -840.12, 434.74]</p>	<p>[(35, 150, 10), (40, 170, 3), (45, 142, 34), (50, 145, 6), (51, 166, 18),]</p>	<p>0110100100100010 0110110001010100 1001111000101000 10011000100100...</p>
<p>Hand feature set: Lengths and widths of fingers, width of palm</p>	<p>Face feature set: Eigen-coefficients</p>	<p>Fingerprint feature set: Minutiae coordinates and local ridge orientation</p>	<p>Iris code: Quantized structure after Gabor filtering</p>
<p>A. Jain - http://www.cse.msu.edu/~cse891/Sect601/Lecture1-4.PDF</p>			<p>© Jain, 2004</p>

Example Data Representations

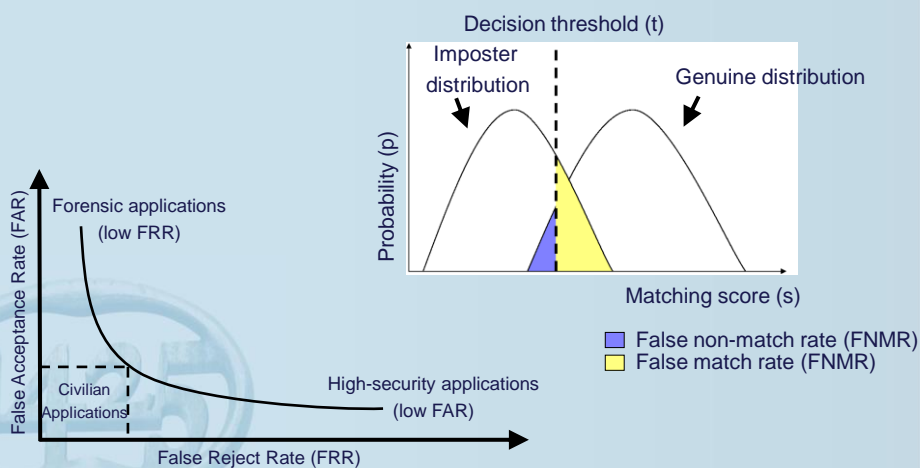
<p>Fixed-length vector</p>  <p>[65 53 59 52 62 4747 45 255 333 253 287 243 149]</p> <p>Hand feature set: Lengths and widths of fingers, width of palm</p>	<p>Fixed-length vector</p>  <p>[-315.91, -441.10, 212.35, -90.78, -840.12, 434.74]</p> <p>Face feature set: Eigen-coefficients</p>	<p>Variable-length 3-tuple</p>  <p>[(35, 150, 10), (40, 170, 3), (45, 142, 34), (50, 110, 15), (55, 130, 20), (60, 160, 25), (65, 180, 30), (70, 200, 35), (75, 220, 40), (80, 240, 45), (85, 260, 50), (90, 280, 55), (95, 300, 60), (100, 320, 65), (105, 340, 70), (110, 360, 75), (115, 380, 80), (120, 400, 85), (125, 420, 90), (130, 440, 95), (135, 460, 100), (140, 480, 105), (145, 500, 110), (150, 520, 115), (155, 540, 120), (160, 560, 125), (165, 580, 130), (170, 600, 135), (175, 620, 140), (180, 640, 145), (185, 660, 150), (190, 680, 155), (195, 700, 160), (200, 720, 165), (205, 740, 170), (210, 760, 175), (215, 780, 180), (220, 800, 185), (225, 820, 190), (230, 840, 195), (235, 860, 200), (240, 880, 205), (245, 900, 210), (250, 920, 215), (255, 940, 220), (260, 960, 225), (265, 980, 230), (270, 1000, 235), (275, 1020, 240), (280, 1040, 245), (285, 1060, 250), (290, 1080, 255), (295, 1100, 260), (300, 1120, 265), (305, 1140, 270), (310, 1160, 275), (315, 1180, 280), (320, 1200, 285), (325, 1220, 290), (330, 1240, 295), (335, 1260, 300), (340, 1280, 305), (345, 1300, 310), (350, 1320, 315), (355, 1340, 320), (360, 1360, 325), (365, 1380, 330), (370, 1400, 335), (375, 1420, 340), (380, 1440, 345), (385, 1460, 350), (390, 1480, 355), (395, 1500, 360), (400, 1520, 365), (405, 1540, 370), (410, 1560, 375), (415, 1580, 380), (420, 1600, 385), (425, 1620, 390), (430, 1640, 395), (435, 1660, 400), (440, 1680, 405), (445, 1700, 410), (450, 1720, 415), (455, 1740, 420), (460, 1760, 425), (465, 1780, 430), (470, 1800, 435), (475, 1820, 440), (480, 1840, 445), (485, 1860, 450), (490, 1880, 455), (495, 1900, 460), (500, 1920, 465), (505, 1940, 470), (510, 1960, 475), (515, 1980, 480), (520, 2000, 485), (525, 2020, 490), (530, 2040, 495), (535, 2060, 500), (540, 2080, 505), (545, 2100, 510), (550, 2120, 515), (555, 2140, 520), (560, 2160, 525), (565, 2180, 530), (570, 2200, 535), (575, 2220, 540), (580, 2240, 545), (585, 2260, 550), (590, 2280, 555), (595, 2300, 560), (600, 2320, 565), (605, 2340, 570), (610, 2360, 575), (615, 2380, 580), (620, 2400, 585), (625, 2420, 590), (630, 2440, 595), (635, 2460, 600), (640, 2480, 605), (645, 2500, 610), (650, 2520, 615), (655, 2540, 620), (660, 2560, 625), (665, 2580, 630), (670, 2600, 635), (675, 2620, 640), (680, 2640, 645), (685, 2660, 650), (690, 2680, 655), (695, 2700, 660), (700, 2720, 665), (705, 2740, 670), (710, 2760, 675), (715, 2780, 680), (720, 2800, 685), (725, 2820, 690), (730, 2840, 695), (735, 2860, 700), (740, 2880, 705), (745, 2900, 710), (750, 2920, 715), (755, 2940, 720), (760, 2960, 725), (765, 2980, 730), (770, 3000, 735), (775, 3020, 740), (780, 3040, 745), (785, 3060, 750), (790, 3080, 755), (795, 3100, 760), (800, 3120, 765), (805, 3140, 770), (810, 3160, 775), (815, 3180, 780), (820, 3200, 785), (825, 3220, 790), (830, 3240, 795), (835, 3260, 800), (840, 3280, 805), (845, 3300, 810), (850, 3320, 815), (855, 3340, 820), (860, 3360, 825), (865, 3380, 830), (870, 3400, 835), (875, 3420, 840), (880, 3440, 845), (885, 3460, 850), (890, 3480, 855), (895, 3500, 860), (900, 3520, 865), (905, 3540, 870), (910, 3560, 875), (915, 3580, 880), (920, 3600, 885), (925, 3620, 890), (930, 3640, 895), (935, 3660, 900), (940, 3680, 905), (945, 3700, 910), (950, 3720, 915), (955, 3740, 920), (960, 3760, 925), (965, 3780, 930), (970, 3800, 935), (975, 3820, 940), (980, 3840, 945), (985, 3860, 950), (990, 3880, 955), (995, 3900, 960), (1000, 3920, 965), (1005, 3940, 970), (1010, 3960, 975), (1015, 3980, 980), (1020, 4000, 985), (1025, 4020, 990), (1030, 4040, 995), (1035, 4060, 1000), (1040, 4080, 1005), (1045, 4100, 1010), (1050, 4120, 1015), (1055, 4140, 1020), (1060, 4160, 1025), (1065, 4180, 1030), (1070, 4200, 1035), (1075, 4220, 1040), (1080, 4240, 1045), (1085, 4260, 1050), (1090, 4280, 1055), (1095, 4300, 1060), (1100, 4320, 1065), (1105, 4340, 1070), (1110, 4360, 1075), (1115, 4380, 1080), (1120, 4400, 1085), (1125, 4420, 1090), (1130, 4440, 1095), (1135, 4460, 1100), (1140, 4480, 1105), (1145, 4500, 1110), (1150, 4520, 1115), (1155, 4540, 1120), (1160, 4560, 1125), (1165, 4580, 1130), (1170, 4600, 1135), (1175, 4620, 1140), (1180, 4640, 1145), (1185, 4660, 1150), (1190, 4680, 1155), (1195, 4700, 1160), (1200, 4720, 1165), (1205, 4740, 1170), (1210, 4760, 1175), (1215, 4780, 1180), (1220, 4800, 1185), (1225, 4820, 1190), (1230, 4840, 1195), (1235, 4860, 1200), (1240, 4880, 1205), (1245, 4900, 1210), (1250, 4920, 1215), (1255, 4940, 1220), (1260, 4960, 1225), (1265, 4980, 1230), (1270, 5000, 1235), (1275, 5020, 1240), (1280, 5040, 1245), (1285, 5060, 1250), (1290, 5080, 1255), (1295, 5100, 1260), (1300, 5120, 1265), (1305, 5140, 1270), (1310, 5160, 1275), (1315, 5180, 1280), (1320, 5200, 1285), (1325, 5220, 1290), (1330, 5240, 1295), (1335, 5260, 1300), (1340, 5280, 1305), (1345, 5300, 1310), (1350, 5320, 1315), (1355, 5340, 1320), (1360, 5360, 1325), (1365, 5380, 1330), (1370, 5400, 1335), (1375, 5420, 1340), (1380, 5440, 1345), (1385, 5460, 1350), (1390, 5480, 1355), (1395, 5500, 1360), (1400, 5520, 1365), (1405, 5540, 1370), (1410, 5560, 1375), (1415, 5580, 1380), (1420, 5600, 1385), (1425, 5620, 1390), (1430, 5640, 1395), (1435, 5660, 1400), (1440, 5680, 1405), (1445, 5700, 1410), (1450, 5720, 1415), (1455, 5740, 1420), (1460, 5760, 1425), (1465, 5780, 1430), (1470, 5800, 1435), (1475, 5820, 1440), (1480, 5840, 1445), (1485, 5860, 1450), (1490, 5880, 1455), (1495, 5900, 1460), (1500, 5920, 1465), (1505, 5940, 1470), (1510, 5960, 1475), (1515, 5980, 1480), (1520, 6000, 1485), (1525, 6020, 1490), (1530, 6040, 1495), (1535, 6060, 1500), (1540, 6080, 1505), (1545, 6100, 1510), (1550, 6120, 1515), (1555, 6140, 1520), (1560, 6160, 1525), (1565, 6180, 1530), (1570, 6200, 1535), (1575, 6220, 1540), (1580, 6240, 1545), (1585, 6260, 1550), (1590, 6280, 1555), (1595, 6300, 1560), (1600, 6320, 1565), (1605, 6340, 1570), (1610, 6360, 1575), (1615, 6380, 1580), (1620, 6400, 1585), (1625, 6420, 1590), (1630, 6440, 1595), (1635, 6460, 1600), (1640, 6480, 1605), (1645, 6500, 1610), (1650, 6520, 1615), (1655, 6540, 1620), (1660, 6560, 1625), (1665, 6580, 1630), (1670, 6600, 1635), (1675, 6620, 1640), (1680, 6640, 1645), (1685, 6660, 1650), (1690, 6680, 1655), (1695, 6700, 1660), (1700, 6720, 1665), (1705, 6740, 1670), (1710, 6760, 1675), (1715, 6780, 1680), (1720, 6800, 1685), (1725, 6820, 1690), (1730, 6840, 1695), (1735, 6860, 1700), (1740, 6880, 1705), (1745, 6900, 1710), (1750, 6920, 1715), (1755, 6940, 1720), (1760, 6960, 1725), (1765, 6980, 1730), (1770, 7000, 1735), (1775, 7020, 1740), (1780, 7040, 1745), (1785, 7060, 1750), (1790, 7080, 1755), (1795, 7100, 1760), (1800, 7120, 1765), (1805, 7140, 1770), (1810, 7160, 1775), (1815, 7180, 1780), (1820, 7200, 1785), (1825, 7220, 1790), (1830, 7240, 1795), (1835, 7260, 1800), (1840, 7280, 1805), (1845, 7300, 1810), (1850, 7320, 1815), (1855, 7340, 1820), (1860, 7360, 1825), (1865, 7380, 1830), (1870, 7400, 1835), (1875, 7420, 1840), (1880, 7440, 1845), (1885, 7460, 1850), (1890, 7480, 1855), (1895, 7500, 1860), (1900, 7520, 1865), (1905, 7540, 1870), (1910, 7560, 1875), (1915, 7580, 1880), (1920, 7600, 1885), (1925, 7620, 1890), (1930, 7640, 1895), (1935, 7660, 1900), (1940, 7680, 1905), (1945, 7700, 1910), (1950, 7720, 1915), (1955, 7740, 1920), (1960, 7760, 1925), (1965, 7780, 1930), (1970, 7800, 1935), (1975, 7820, 1940), (1980, 7840, 1945), (1985, 7860, 1950), (1990, 7880, 1955), (1995, 7900, 1960), (2000, 7920, 1965), (2005, 7940, 1970), (2010, 7960, 1975), (2015, 7980, 1980), (2020, 8000, 1985), (2025, 8020, 1990), (2030, 8040, 1995), (2035, 8060, 2000), (2040, 8080, 2005), (2045, 8100, 2010), (2050, 8120, 2015), (2055, 8140, 2020), (2060, 8160, 2025), (2065, 8180, 2030), (2070, 8200, 2035), (2075, 8220, 2040), (2080, 8240, 2045), (2085, 8260, 2050), (2090, 8280, 2055), (2095, 8300, 2060), (2100, 8320, 2065), (2105, 8340, 2070), (2110, 8360, 2075), (2115, 8380, 2080), (2120, 8400, 2085), (2125, 8420, 2090), (2130, 8440, 2095), (2135, 8460, 2100), (2140, 8480, 2105), (2145, 8500, 2110), (2150, 8520, 2115), (2155, 8540, 2120), (2160, 8560, 2125), (2165, 8580, 2130), (2170, 8600, 2135), (2175, 8620, 2140), (2180, 8640, 2145), (2185, 8660, 2150), (2190, 8680, 2155), (2195, 8700, 2160), (2200, 8720, 2165), (2205, 8740, 2170), (2210, 8760, 2175), (2215, 8780, 2180), (2220, 8800, 2185), (2225, 8820, 2190), (2230, 8840, 2195), (2235, 8860, 2200), (2240, 8880, 2205), (2245, 8900, 2210), (2250, 8920, 2215), (2255, 8940, 2220), (2260, 8960, 2225), (2265, 8980, 2230), (2270, 9000, 2235), (2275, 9020, 2240), (2280, 9040, 2245), (2285, 9060, 2250), (2290, 9080, 2255), (2295, 9100, 2260), (2300, 9120, 2265), (2305, 9140, 2270), (2310, 9160, 2275), (2315, 9180, 2280), (2320, 9200, 2285), (2325, 9220, 2290), (2330, 9240, 2295), (2335, 9260, 2300), (2340, 9280, 2305), (2345, 9300, 2310), (2350, 9320, 2315), (2355, 9340, 2320), (2360, 9360, 2325), (2365, 9380, 2330), (2370, 9400, 2335), (2375, 9420, 2340), (2380, 9440, 2345), (2385, 9460, 2350), (2390, 9480, 2355), (2395, 9500, 2360), (2400, 9520, 2365), (2405, 9540, 2370), (2410, 9560, 2375), (2415, 9580, 2380), (2420, 9600, 2385), (2425, 9620, 2390), (2430, 9640, 2395), (2435, 9660, 2400), (2440, 9680, 2405), (2445, 9700, 2410), (2450, 9720, 2415), (2455, 9740, 2420), (2460, 9760, 2425), (2465, 9780, 2430), (2470, 9800, 2435), (2475, 9820, 2440), (2480, 9840, 2445), (2485, 9860, 2450), (2490, 9880, 2455), (2495, 9900, 2460), (2500, 9920, 2465), (2505, 9940, 2470), (2510, 9960, 2475), (2515, 9980, 2480), (2520, 10000, 2485), (2525, 10020, 2490), (2530, 10040, 2495), (2535, 10060, 2500), (2540, 10080, 2505), (2545, 10100, 2510), (2550, 10120, 2515), (2555, 10140, 2520), (2560, 10160, 2525), (2565, 10180, 2530), (2570, 10200, 2535), (2575, 10220, 2540), (2580, 10240, 2545), (2585, 10260, 2550), (2590, 10280, 2555), (2595, 10300, 2560), (2600, 10320, 2565), (2605, 10340, 2570), (2610, 10360, 2575), (2615, 10380, 2580), (2620, 10400, 2585), (2625, 10420, 2590), (2630, 10440, 2595), (2635, 10460, 2600), (2640, 10480, 2605), (2645, 10500, 2610), (2650, 10520, 2615), (2655, 10540, 2620), (2660, 10560, 2625), (2665, 10580, 2630), (2670, 10600, 2635), (2675, 10620, 2640), (2680, 10640, 2645), (2685, 10660, 2650), (2690, 10680, 2655), (2695, 10700, 2660), (2700, 10720, 2665), (2705, 10740, 2670), (2710, 10760, 2675), (2715, 10780, 2680), (2720, 10800, 2685), (2725, 10820, 2690), (2730, 10840, 2695), (2735, 10860, 2700), (2740, 10880, 2705), (2745, 10900, 2710), (2750, 10920, 2715), (2755, 10940, 2720), (2760, 10960, 2725), (2765, 10980, 2730), (2770, 11000, 2735), (2775, 11020, 2740), (2780, 11040, 2745), (2785, 11060, 2750), (2790, 11080, 2755), (2795, 11100, 2760), (2800, 11120, 2765), (2805, 11140, 2770), (2810, 11160, 2775), (2815, 11180, 2780), (2820, 11200, 2785), (2825, 11220, 2790), (2830, 11240, 2795), (2835, 11260, 2800), (2840, 11280, 2805), (2845, 11300, 2810), (2850, 11320, 2815), (2855, 11340, 2820), (2860, 11360, 2825), (2865, 11380, 2830), (2870, 11400, 2835), (2875, 11420, 2840), (2880, 11440, 2845), (2885, 11460, 2850), (2890, 11480, 2855), (2895, 11500, 2860), (2900, 11520, 2865), (2905, 11540, 2870), (2910, 11560, 2875), (2915, 11580, 2880), (2920, 11600, 2885), (2925, 11620, 2890), (2930, 11640, 2895), (2935, 11660, 2900), (2940, 11680, 2905), (2945, 11700, 2910), (2950, 11720, 2915), (2955, 11740</p>
--	---	---

Desired Properties

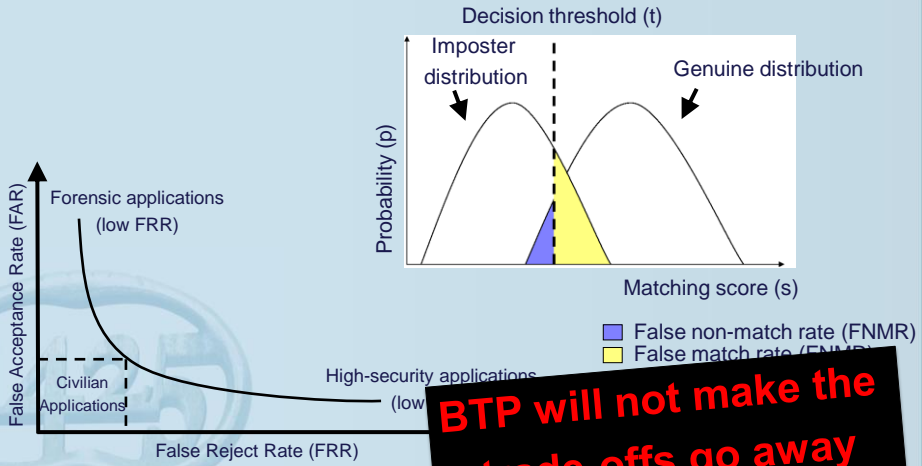
Biometrics	Face	Fingerprint	Hand Geometry	Iris	Retinal Scan	Signature	Voice Print	Facial Thermogram
Universality	high	medium	medium	high	high	low	medium	high
Uniqueness	low	high	medium	high	high	low	low	high
Permanence	medium	high	medium	high	medium	low	low	low
Collectability	high	medium	high	medium	low	high	medium	high
Performance	low	high	medium	high	high	low	low	medium
Acceptability	high	medium	medium	low	low			
Circumvention	low	high	medium	high	high			

Permanence vs. Revocation

Biometric Error Rates



Biometric Error Rates



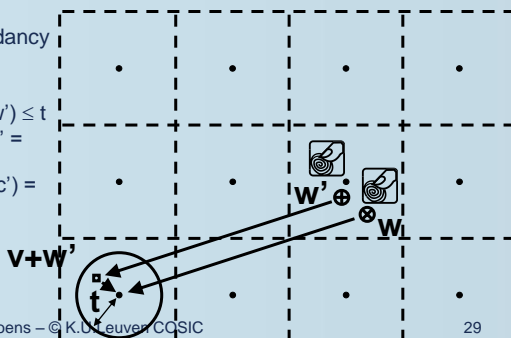
BTP will not make the trade-offs go away



Examples and Standardization

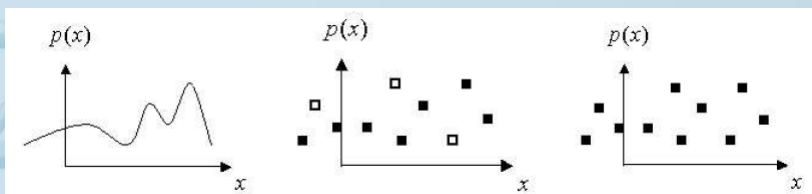
Code-Offset Construction

- Introduced as the **fuzzy commitment** scheme
 - Juels and Wattenberg (1999)
- Enrolment
 - Output and store $v = c - w$ and $H(c)$
 - c is a codeword of an $[n, k, d]$ -code chosen uniformly at random
 - H is a cryptographic hashing function
 - **Entropy loss = $n - k$** (redundancy bits)
- Verification
 - $\text{Dec}(v + w') - v = w$ iff $\text{dis}(w, w') \leq t$
 - Fuzzy commitment outputs $c' = \text{Dec}(v+w)$
 - Verification by comparing $H(c') = H(c)$



Fuzzy Vault

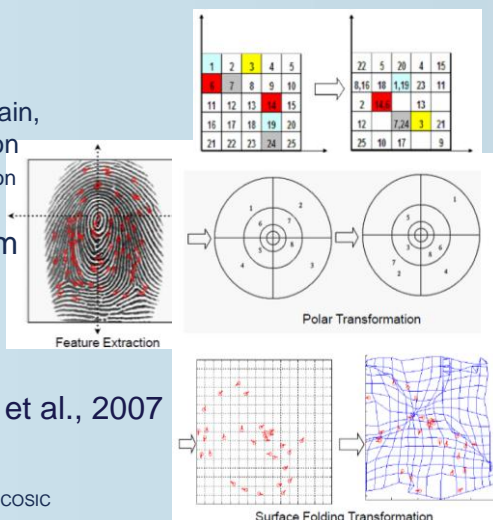
- Juels and Sudan 2002
 - Enrolment data is subset of some universe
 - Verification data must overlap substantially with enrolment data
- Based on polynomial secret sharing
 - Enroll unordered data set as points on polynomial
 - Biometric features as indices for points on $p(x)$
 - Add “**chaff points**” (not on the polynomial)
 - Verification = reconstruction of polynomial and secret



Uludag & Jain, 2005. Fuzzy Vault for Fingerprints

Cancelable Biometrics

- 31 • Ratha et al. 2001, 2007
- Intentional repeatable distortion
 - In signal or feature domain, preserving representation
 - Reuse existing comparison algorithms
- Non-invertible transform



Ratha et al., 2007

Koen Simoens – © K.U.Leuven COSIC
LSEC Biometrics 2011

The Need for a Standardized Definition

- Observe:
 - Many different BTP schemes in literature
 - Different data representations in biometrics
- Where to apply protection? (how to model)



Minutiae

88 237 247 15
92 109 180 35
100 141 180 71
101 228 101 16
...

10111011001...



LSEC Biometrics 2011

Koen Simoens – © K.U.Leuven COSIC

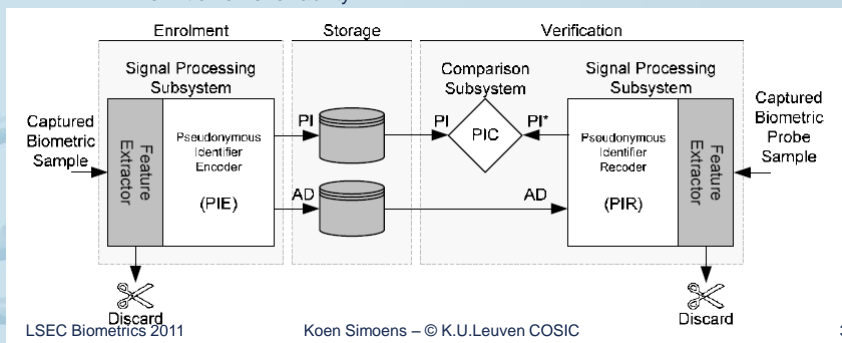
32

ISO 24745

- ISO/IEC 24745. (2011). Information technology - Security techniques - Biometric information protection.
 - Stage 60.60: International Standard published
 - Heavily influenced by the TURBINE project
 - <http://www.turbine-project.eu>
 - A reference architecture for biometric template protection
- Main elements of the architecture
 - Data elements
 - Functional components
- Many schemes mapped on the architecture

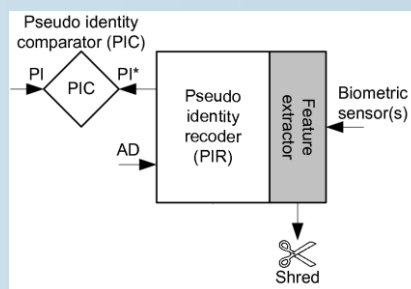
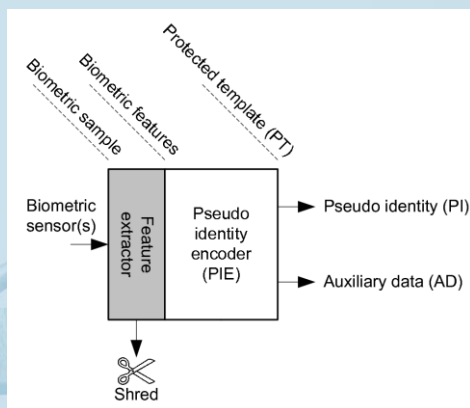
Reference Architecture

- Data units
 - Pseudonymous Identifier (PI)
 - Auxiliary Data (AD)
 - Protected Template (PT) = PI and AD
 - Synonym for renewable biometric template
 - Definition of renewability



Functional Components

- Pseudonymous Identifier Encoder (PIE)
- Pseudonymous Identifier Recoder (PIR)
- Pseudonymous Identifier Comparator (PIC)



Example Mappings

Method	PI	AD
Helper data systems	Hash of secret string	Helper data
Fuzzy commitment	Hash of secret string	Offset
Biometric encryption	Cryptographic key	Filter and key link
Fuzzy vault	Hash of secret string	Point set P
Shielding functions	Hash of secret string	Authentication challenge W
Fuzzy extractors	Hash of secret string	Public string P
Extended PIR	Encrypted template	n/a
2D hexagonal quantization index modulation	Hash of a secret string	Quantization errors
Cancellable biometrics	Transformed template	Transform parameters
Biometric robust hashing	Hash of a robust binary string	One-way transformation
Biohashing	A robust binary string	Random projection matrix
Short-lived cryptokey	Crypto-keys	System parameters
Bio-tokens	Encrypted minutiae	Cryptographic keys
Secure sketch	Quantization residue	Quantizer
Robust minutiae hash	Robust binary string for each minutia	Random diversification table



Evaluating BTP

Current Research Challenges

- Many different BTP schemes in literature
 - **Lack of well-established metrics** for evaluating BTP methods
 - Proper evaluation or direct comparison not possible
- Develop **metrics for ranking and independent benchmarking**
 - Project Partners
 - KUL : Katholieke Universiteit Leuven, COSIC – Belgium
 - GUC : Gjøvik University College, NISlab – Norway
 - Previous collaboration in **TURBINE project** (EU-funded, 3 year)
 - Protected biometric (fingerprint) identities
 - Independent evaluators (security/privacy and technical performance)
 - Decision to extend our work under the support of NIST (USA)

Objectives

- Identification and selection of criteria that are relevant for BTP method evaluation
 - What are the key properties to assess?
- Harmonized definitions
 - How to define them consistently w.r.t. the reference architecture?
- Focus on criteria directly related to BTP
- Target criteria that are quantifiable or measurable in a precise way
 - Not trying to measure user acceptance
- Categorize in three performance groups:
 - Technical, security and privacy, operational performance
- Challenge
 - Try to come up with universal metrics that can be empirically evaluation
- Results to be presented at ICB 2012
 - *“Metrics for benchmarking template protection”*

Evaluation Criteria

Technical performance:

- Accuracy
- Accuracy degradation
- Throughput
 - PI encoding time
 - PI recoding time
 - PI comparison time
- Storage requirements
 - Protected template size
 - Code size
- Diversification capacity

Security and privacy performance:

- Full-leakage irreversibility
- Authorized-leakage irreversibility
- Pseudo-authorized-leakage irreversibility
- Unlinkability

Operational performance:

- Modality independence
- Interoperability
- Quality of performance (QoP)
 - Granularity of performance
 - Stability of performance



Conclusion

Expectations for The Future

- Different biometrics and different protection methods
 - To a large extent determined by the application
 - **Data representation has an impact**
- Each protection mechanisms has to be analyzed differently
 - Need for harmonized evaluation criteria and metrics
 - Less “we think/believe...”
 - NIST collaboration platform
 - <http://collaborate.nist.gov/wiki-secbiotemp/>
- Biometric template protection has yet to mature
 - More **secure techniques** are needed
 - Performance is an issue (not discussed in this talk)
 - So far **provable security** in biometrics is non-existing



Thank you!

koen.simoens@esat.kuleuven.be

References

- Books
 - Jain, A. K., Flynn, P., & Ross, A. A. (2008). Handbook of Biometrics. Springer.
 - Tuyls, P., Boris Škorić, Kevenaar, T. (Eds.) (2007). Security with Noisy Data: Private Biometrics, Secure Key Storage and Anti-Counterfeiting. Springer.
 - Li, S. & Jain, A. (Eds) (2011). Encyclopedia of Biometrics. Springer.
 - Adam Davison Smith: Maintaining Secrecy when Information Leakage is Unavoidable, Massachusetts Institute of Technology, August 2004 (Doctoral thesis)
- Introductory
 - Jain, A., Hong, L., & Pankanti, S. (2000). Biometric Identification. Communication of the ACM , 43(2), pp. 91-98.
 - Prabhakar, S., Pankanti, S., & Jain, A. (2003). Biometric Recognition: Security and Privacy Concerns. IEEE Security and Privacy , 1 (2), pp. 33-42.
- Models
 - Jean-Paul M. G. Linnartz, and Pim Tuyls (2003). New Shielding Functions to Enhance Privacy and Prevent Misuse of Biometric Templates, AVBPA, 393-402
 - Yevgeniy Dodis, Leonid Reyzin, and Adam Smith (2004). Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data, Advances in Cryptology - EUROCRYPT 2004, 523-540

References

- Selected methods for template protection
 - Ari Juels, and Martin Wattenberg: A fuzzy commitment scheme (1999), CCS '99: Proceedings of the 6th ACM conference on Computer and communications security, ACM Press, 28-36
 - Ratha, N. K., Connell, J. H., & Bolle, R. M. (2001). Enhancing security and privacy in biometrics-based authentication systems. *IBM Systems Journal*, 40 (3), 614-634.
 - Juels, A. & Sudan, M. (2002). A Fuzzy Vault Scheme. Proc. of IEEE International Symposium on Information Theory, p.408.
 - Tuyls, P., Akkermans, A.H.M., Kevenaer, T.A. M., Schrijen, G.J., Bazen, A.M., & Veldhuis, R.N.J. (2005). Practical Biometric Authentication with Template Protection, AVBPA, 436-446
 - Uludag, U., Pankanti, S. & Jain, A.K. (2005). Fuzzy vault for fingerprints. Proc. AVBPA, LNCS 3546. pp.310–319
 - Ratha, N. K., Chikkerur, S., Connell, J. H., & Bolle, R. M. (2007). Generating Cancelable Fingerprint Templates. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 29 (4), pp. 561 - 572.
 - Bringer, J., Chabanne, H., Kevenaer, T. A., & Kindarji, B. (2009). Extending Match-On-Card to Local Biometric Identification. *COST 2 101/2 102*, (pp. 178-186).
 - Kelkboom, E., Breebaart, J., Kevenaer, T. A., Buhan, I., & Veldhuis, R. N. (2011). Preventing the Decodability Attack based Cross-matching in a Fuzzy Commitment Scheme. Information Forensics and Security, IEEE Transactions on , 15 pages, accepted for publication.

References

- Security analysis
 - Jain, A. K., Nandakumar, K., and Nagar, A. 2008. Biometric template security. *EURASIP J. Adv. Signal Process* 8, 2, pp. 1-17.
 - Simoens, K., Tuyls, P., and Preneel, B. 2009. Privacy weaknesses in biometric sketches. In Proc. of the 2009 30th IEEE Symposium on Security and Privacy, 188-203.
 - J. Bringer, H. Chabanne, and K. Simoens. 2010. Blackbox Security of Biometrics (invited paper). In International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP 2010), IEEE, pp. 337-340.
 - Koen Simoens, Julien Bringer, Hervé Chabanne, Stefaan Seys (2011). Analysis of Biometric Authentication Protocols in the Blackbox Model. arXiv:1101.2569
- Standards
 - ISO/IEC 19795-1, (2006). Information technology - Biometric performance testing and reporting - Part 1: Principles and framework.
 - ISO/IEC TR 24741. (2007). Information technology - Biometrics Tutorial.
 - ISO/IEC 24760-1. (2010). Information technology - Security techniques – A framework for identity management -- Part 1: Terminology and concepts.
 - ISO/IEC CD 2382-37. (2010). JTC1/SC 37 Standing Document 2 (SD 2) version 11, Harmonized Biometric Vocabulary.
 - ISO/IEC 24745. (2011). Information technology - Security techniques - Biometric information protection.

References

- Risk Management and Certification
 - Cukic, B., & Bartlow, N. (2005). Biometric System Threats and Countermeasures: a Risk Based Approach. Proc. of the 2005 Biometric Consortium Conference .
 - ENISA (European Network and Information Security Agency). (2005). Inventory of Risk Management / Risk Assessment Methods.
 - http://www.enisa.europa.eu/mra/rm_ra_methods.html
 - CCRA (Common Criteria Recognition Agreement). (2006). Common Criteria for Information Technology Security Evaluation. Part 1. Introduction and general model. Version 3.1, revision 1.
 - <http://www.commoncriteriaportal.org/thecc.html>
 - BSI (Bundesamt für Sicherheit in der Informationstechnik). (2008). Biometric Verification Mechanisms Protection Profile Version 1.3.
 - <http://www.commoncriteriaportal.org/files/ppfiles/pp0043b.pdf>
 - IAD (Information Assurance Directorate). (2007, Version 1.1). U.S. Government Biometric Verification Mode Protection Profile for Basic Robustness Environments.
 - http://www.commoncriteriaportal.org/files/ppfiles/pp_bvm_br_v1.1.pdf
 - IAD (Information Assurance Directorate). (2007, Version 1.1). U.S. Government Biometric Verification Mode Protection Profile for Medium Robustness Environments.
 - http://www.commoncriteriaportal.org/files/ppfiles/pp_bvm_mr_v1.1.pdf