



TRZYDZIESTE  
**FORUM**  
TELEINFORMATYKI®

# System umożliwiający utworzenie cyfrowej tożsamości z wykorzystaniem procedury dowodu z wiedzy zerowej

Autor: Mgr inż. Bartłomiej Garbacz

Opiekun naukowy : Płk dr inż. Rafał Kasprzyk

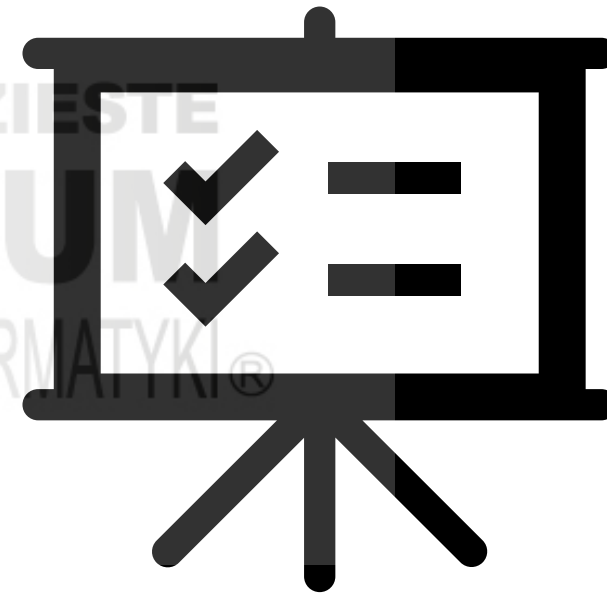
Problematyka

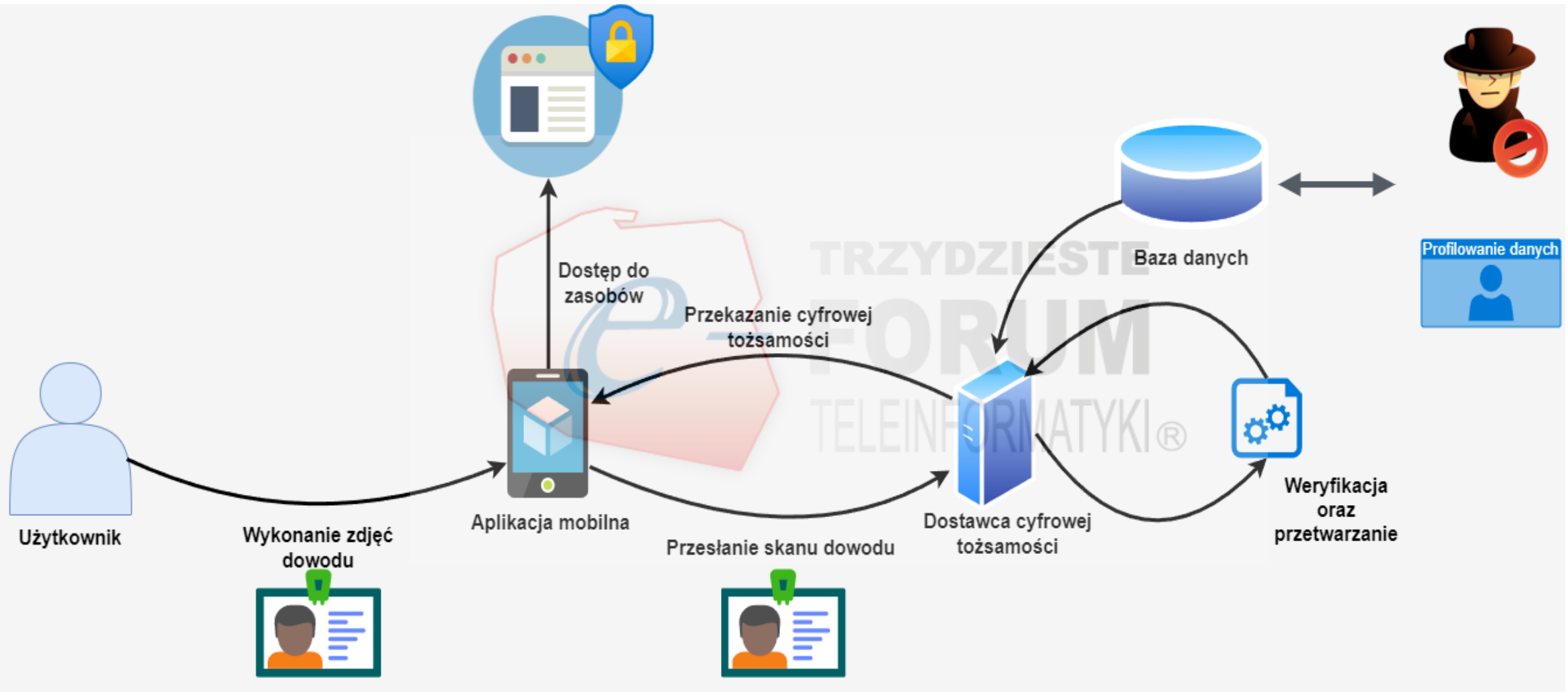
Dowód z wiedzy zerowej – czym właściwie jest?

Rozwiązanie - architektura

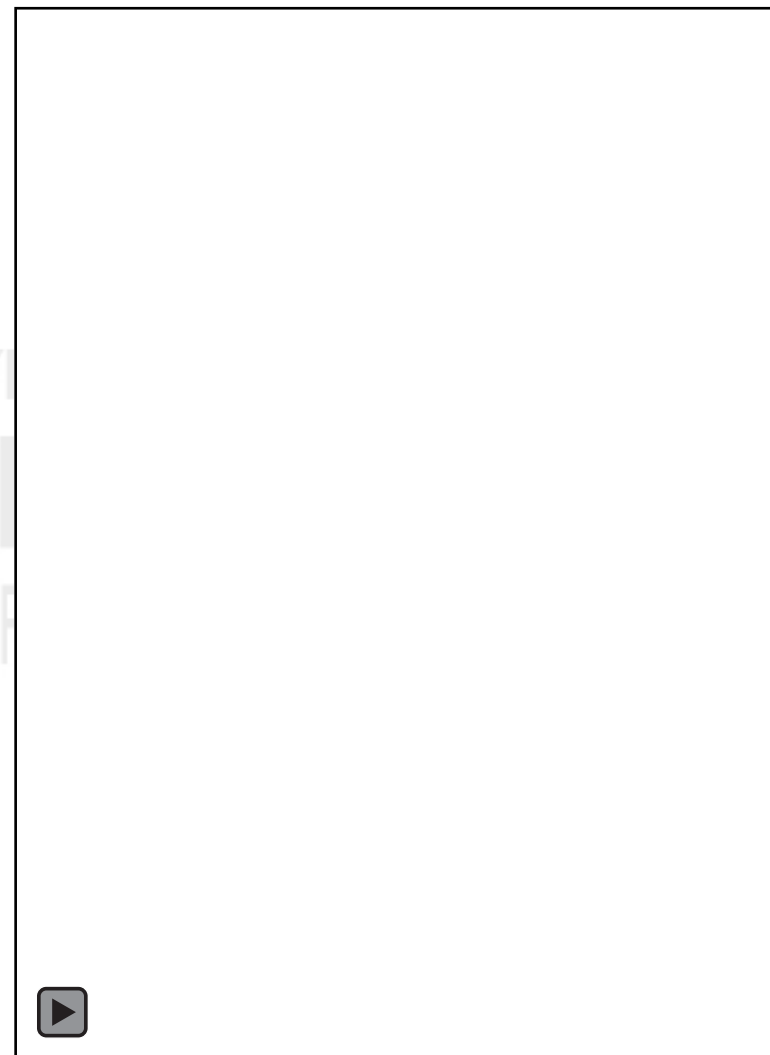
Prezentacja rozwiązania

Dalszy rozwój

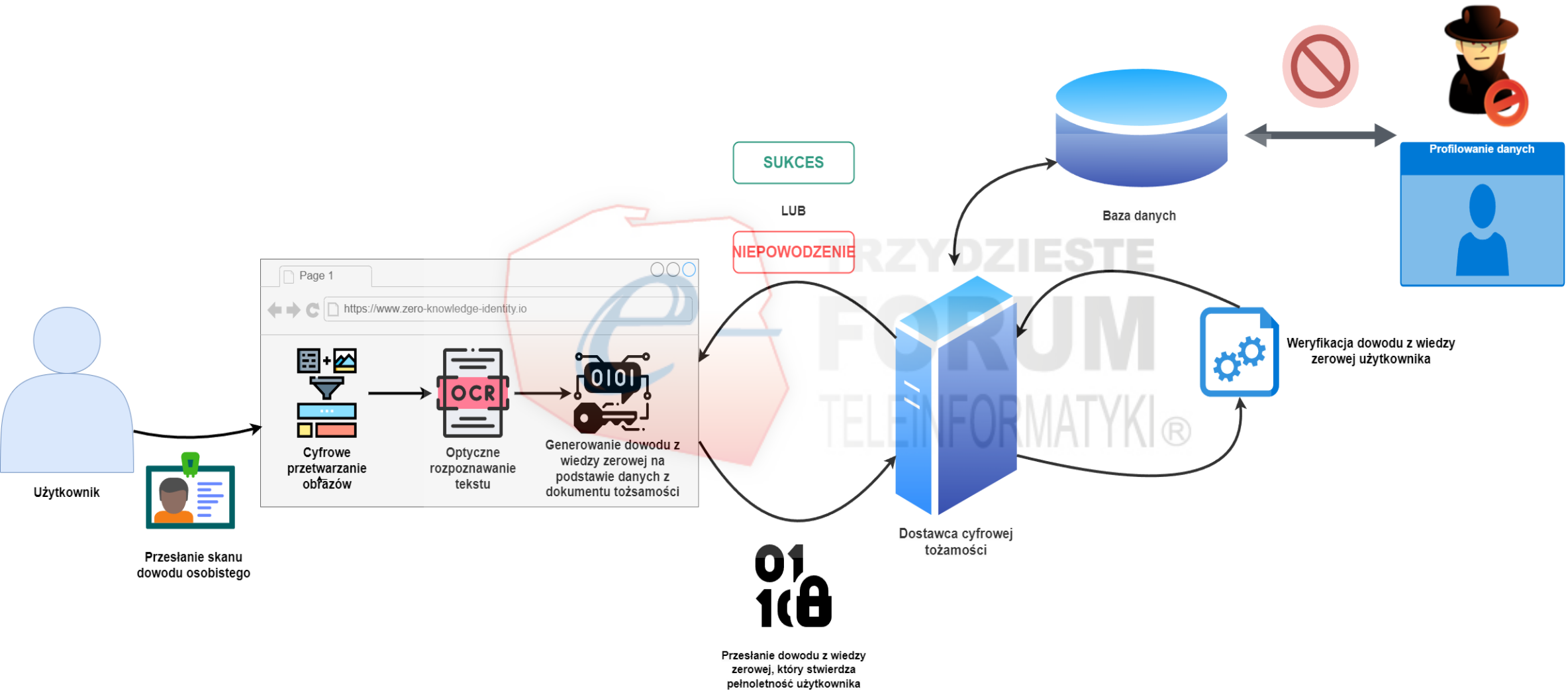


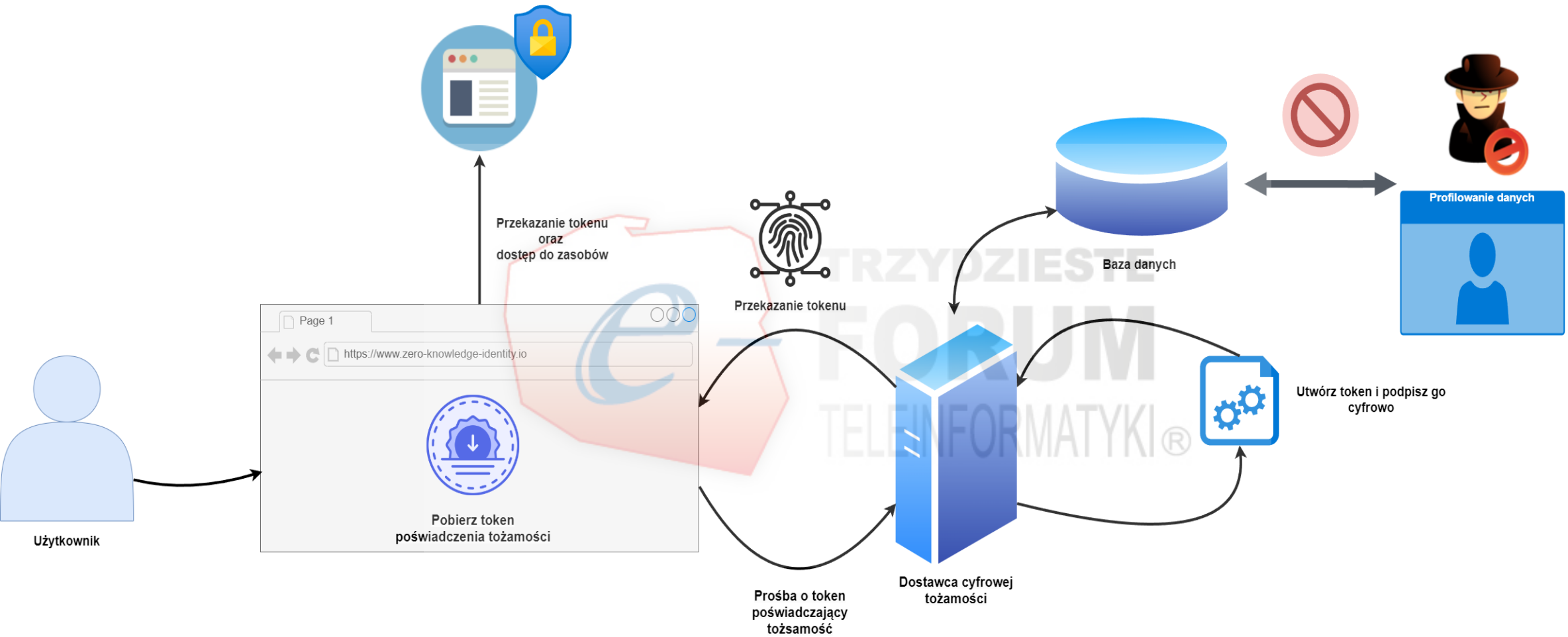


żabka









# Prezentacja rozwiązania

```
hash : 1471d6b79531010652fa185eeda2c87a329ad7610d6d84f62e362fc4ae3f67f1
date_of_birth : 895528800
expiry_date : 1779487200
proof : tt9z0s1-z1-RWJ4Boodh_1dd1W-
gT7YzrxpgePHleLRT0wqoQUBxHYHx_9hPpZ00uJyCwFmH51y7n7Z6URQrvKXCdNca1Kbo1Vwvz4_Uei0i0Y_F3swbAkIpeGnuEhrpHCXRTkd4vi1fiqPjPInDZ4hocFdZU-
uTI0Mvh3Fslwb0Gp8aeTzmy-iquaZ-s4QlqqSntIXdZ13JwR0T12clqGimFfj-XUyEioQEbpgHlUPR8C1yMboXRcrLjji7
verifying_key : FtovWeLHWzL6XxcvoIgfLlTepRigQ3sVQ4BXIZv9ainMatBUydbb1t767wX8T1C3Bn8eKFI5LvaAq4i4C87aLi6BhJ1-
w10AvMf4FZ_61L4DqgQLFB0U13CmPyXvU7DAAZRFMLXYRxcjUru-uZ0n8XGXG72v1EBkWhQD3B7w8fj9F55S3ImxPdH1Rsubbz8mD57N-
UZxkce3Qit8WJCi0tV9wupcjSvArtjQbX4QUBER0D1B95exV7tbH6LH_1VoGSRKjoht26H1MML_Z5sIMBkhnAfSVUvNYtJriuiGPEps0_y1-
1Kx011wotjlnhN2CpmLa38yPz0Tj-s1xRqAC1kA-oQ2SbrgVhgw0ukz7Y8nzFtAEBTbvtznc1qkbb1AR1G-
91bM3v6c22nBvdGqVB0qrthF2NLHkxtxhwXwi06VexRU4djx05VFRVrdYwsA7FPZu4iF5V3sd9q12tDHksifOVfdVwubw29cbw_2T21Y50IdIKXy5u0R14DRDtEBGZi77
RktXRHEfc4EyxUxp90BrN8r4uteRHp1k08R-3_cme1ExkeRT-
viQJufQACwAieZYxDPYGipjaincyfsASIRa0t7NCwcIlpn5e33s04yx_r0XR47TF9hIP60A090AZN7FRZUmUgFDrnxDlkd3DN0-cEoV-
fs95qyR5bjUbhyWouPkt9CAI4N3AwYB_t9hK1McCpX9_hCN2ggJ43t2912878R07mg3JxVjTuokIqC011syuqnrkMvRQF4PaVkj0trQidiNiuUa7ehyBRdtCU10Avtk
6Dhqim-94RRITbkuuzXeT1JnoqpkA_T6XGwYi72zIQj1Dp3E43pfGe_A91111jD6yuq1xS4XIPiNH9rbzaBe0aF--
EYCW0Isp08MeAw9NzuZjphr7nxXsXduM90xAcHwb1-YjghM1rtpwFQ08MOrkFA0enNarf-
xXBcYsopUgJjAxbQysJotd3g459vVyAtuBcQo11yMtnR3Xhw_jKxVuXeYxy_yvFc8Ai-XbwM79KBfKBQvcu453JkWXDxcR0QCh18YPpE5o9DXz_OhTxiLbn2pf7t4-
sMTh0-HwoY0eodNvnCk8ysfSKwqJiy_sHG3jQV_04nq-
Ifq04nPW6EMAAAB0Qt6tCMfnXORxOKRT0C8E313tpHdnMnPhEEI2IjsbaStIft9iqUC8dQyJeTrvV8QLACN1xm2d4EuQ1hPTH1f-DqXmXkIqTL5ysr-
5ki0iIncaystbauHwe-Z56EGtAD2tMtQujwAb2E-ndA2U1J1RKL1trYXKsAnYB-
Nx1P6s5ym7WRckw_0x5buFy22dAGIZLo_IwclUrDchcsmF3pPa950VGnnJ1ZosgytKeccdNV21DL-
9ukvLzCm7w9iAFvklVlWnQpw7zxb1Sjoc4JpHu_BseA6I8U7qRSCc9C5ifiYHaQkUxq0aIzigTdpw4bL66D_Smlq12jr0otE_7gUaUwXhce1QskAUU05A5Sg0ji5i3
eNKJZ-
DDW9grXqo_Uplpzd7TDnmyI4xHu9vbpF3PxdU6ZpvYeZt6KUKBMOTX77jclpxYS8FymQhn6423jGu9ArEC11jNSR4HzDNCwiZDB1u4BAM163H3Lvp1obUkmAoU8C4Cuq-
GTAwQrXcma1BdfjhZ24UCuMkt6Wfe3Az1vAb5sY74MEPDQ3hNDDBHEC0M1HoyJQmVoAaC-A7isMr1XR7P1wsVBIn_HHry4iKfBl1ADSEzUI10eWB-
FoTW7mJGRexSxIm4jw==
```



Utworzenie aplikacji mobilnej;

Integracja z technologią Intel SGX, a w tym:

Przeniesienie obliczeń generowania dowodu z wiedzy zerowej w chmurze zamieszczając kod w odizolowanej enklawie;

Dodatkowa weryfikacja zdjęcia twarzy wraz ze zdjęciem dowodu osobistego zamieszczając kod w odizolowanej enklawie;

Dodanie opcji utworzenia kodu QR dla tokenu potwierdzającego tożsamość;