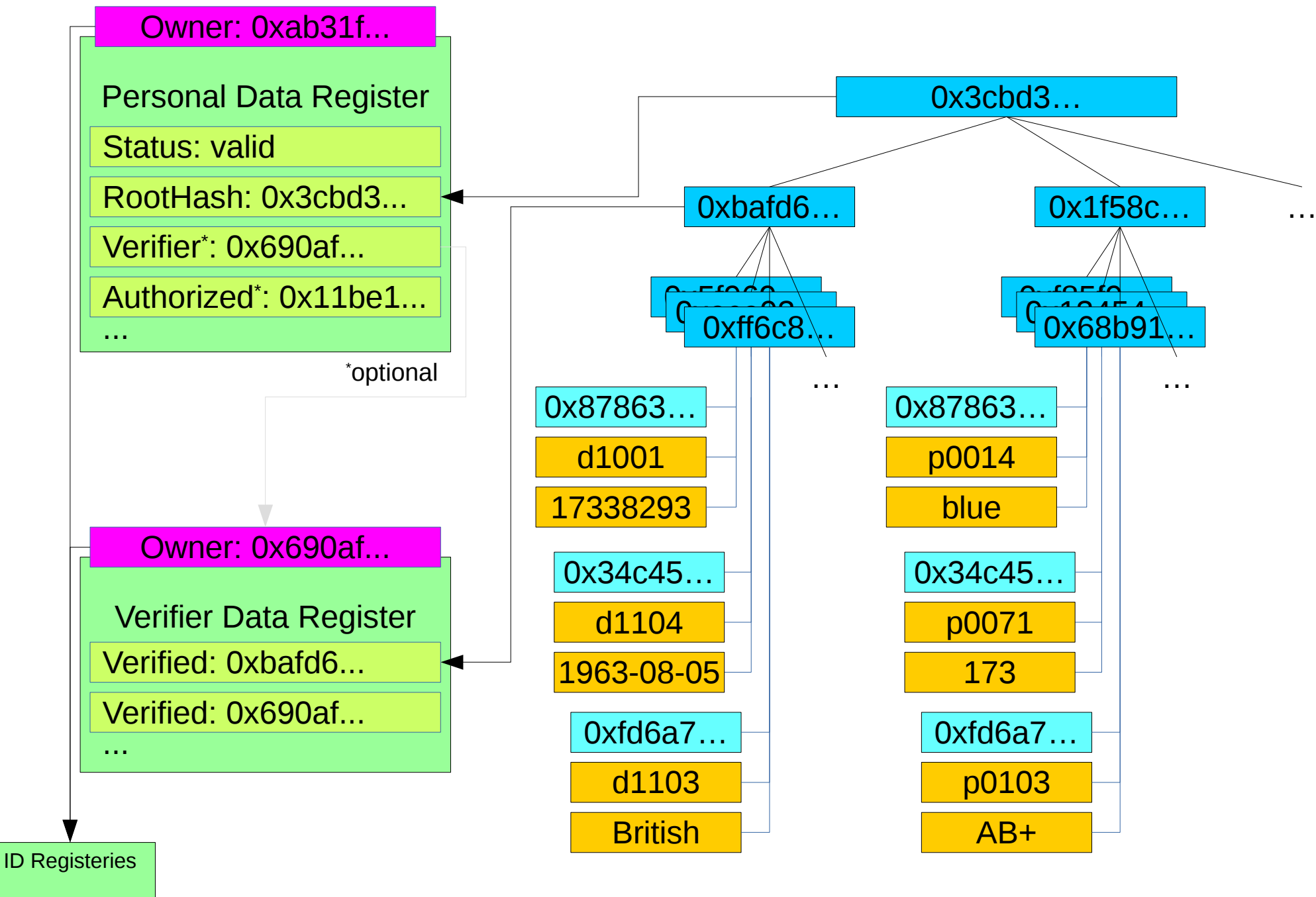


SPDV: Simple Personal Data Verification on Open Blockchains

Author: Aeron Buchanan. Version 1. Released under the [Creative Commons Attribution-ShareAlike license](https://creativecommons.org/licenses/by-sa/4.0/).

On-chain
(smart contracts)

Off-chain
(no personal data, even hashed data, ever goes on-chain)



SPDV: Simple Personal Data Verification on Open Blockchains

Author: Aeron Buchanan. Version 1. Released under the [Creative Commons Attribution-ShareAlike license](https://creativecommons.org/licenses/by-sa/4.0/).

Verification Procedure
Example: Date of Birth

1. Requestor asks for DoB
2. Applicant provides:
 - i. Personal Data Register
 - ii. DoB data & salt
 - iii. Hash tree entries
 - iv. Optionally: Verifier (if not in PDR)
3. Requestor checks:
 - i. Applicant public key (revoked or black-listed?)
 - ii. Verifier public key
 - iii. Hash chain
 - iv. Root hash(es)
 - v. Item code

Note: could just be year or an “over 18” flag

Advantages:

1. No resources required of Verifier
2. Signature of Applicant not required
3. Remote verification possible
4. Selective data release

Future: superceded by secret sharing

