MODELING OF THE ONLINE VOTING SYSTEM OVOTE VIA COMPONENTS

OVOTE: ONLINE VOTING SYSTEM

Characteristics:

- High availability
- Anonymity
- Prevent multiple votes

Amazon Elastic Cloud Computing
- Cross-platform
- Low cost
- Robust API
- Secure

Amazon DynamoDB
- Predictable performance
- Distributed database
- Stored using SSD

Disjoint the voter of the ballot
- The ballot is not stored at DB

Use of local cache
- First search in the cache if the voter already voted
- Reduce the DynamoDB queries

Use of Components

OVOTE must be seen as a service that:

- Each instance provides the same service
- A vote must not affect other votes

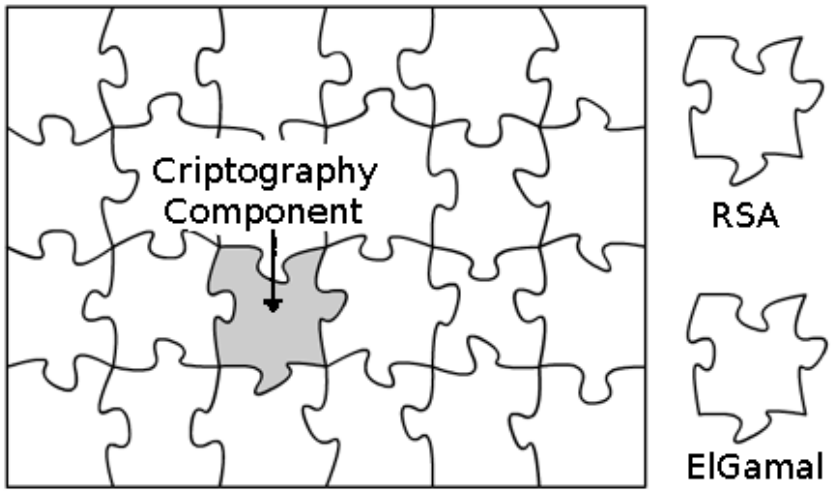
Hence, we can prescind from internal state

- Cache is not considered an internal state because it can be removed at any time without affecting the result

Component Based Methodology

David Lundin propose a component based methodology for developing electronic voting systems

- Build the system adding certain distinct pieces together.
- In order to improve on a particular feature, swap one distinct piece for another that fits into the same slot.
- With the verifiability of each component can show that the full system is verifiable.
- Threat analysis attached to each componenet.



Lundin's Component Hierarchy

1. **Physical Layer**
2. **Computation Layer**
3. **Election Layer**
4. **Human Layer**

- Authenticity
- Anonymity
- Unique vote verification
- Tallying procedure

- High availability
- Efficiency
- Auditable

Grid Component Model

GCM: Component model to support the development of efficient grid application

- Grid computing
- Parallelisms and distribution
- Cover large geographical distances
- Low-cost

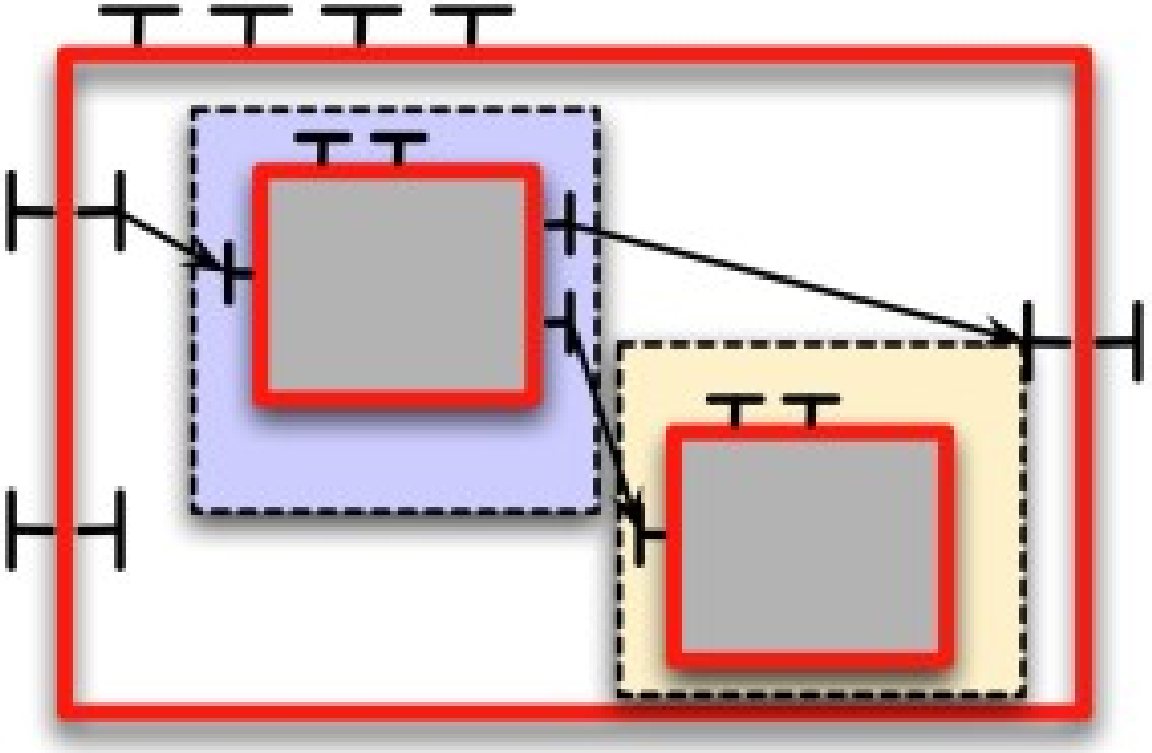
ProActive/GCM: provides a implementation of the GCM

ProActive/GCM

Support the development of grid applications abstracting away grid related implementation details

- Creation/usage of primitive and composite components
- Client, Server and non-functional interfaces
- Multicast and gathercast Interfaces
- Several componenets in and assembly can be distributed on several computers

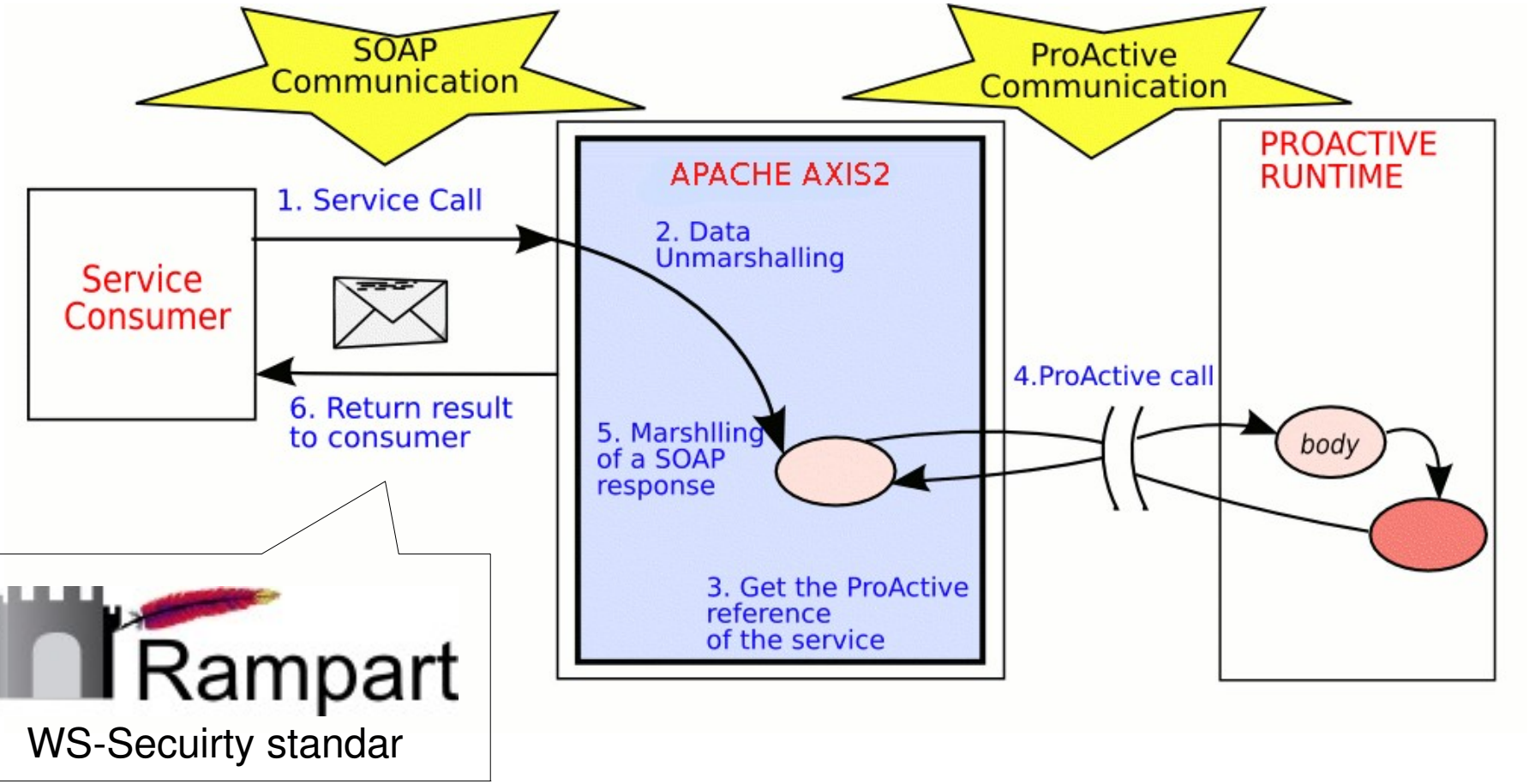
ProActive/GCM



A system of distributed ProActive/GCM components
(blue, yellow and white represent distinct locations)

ProActive/CGM

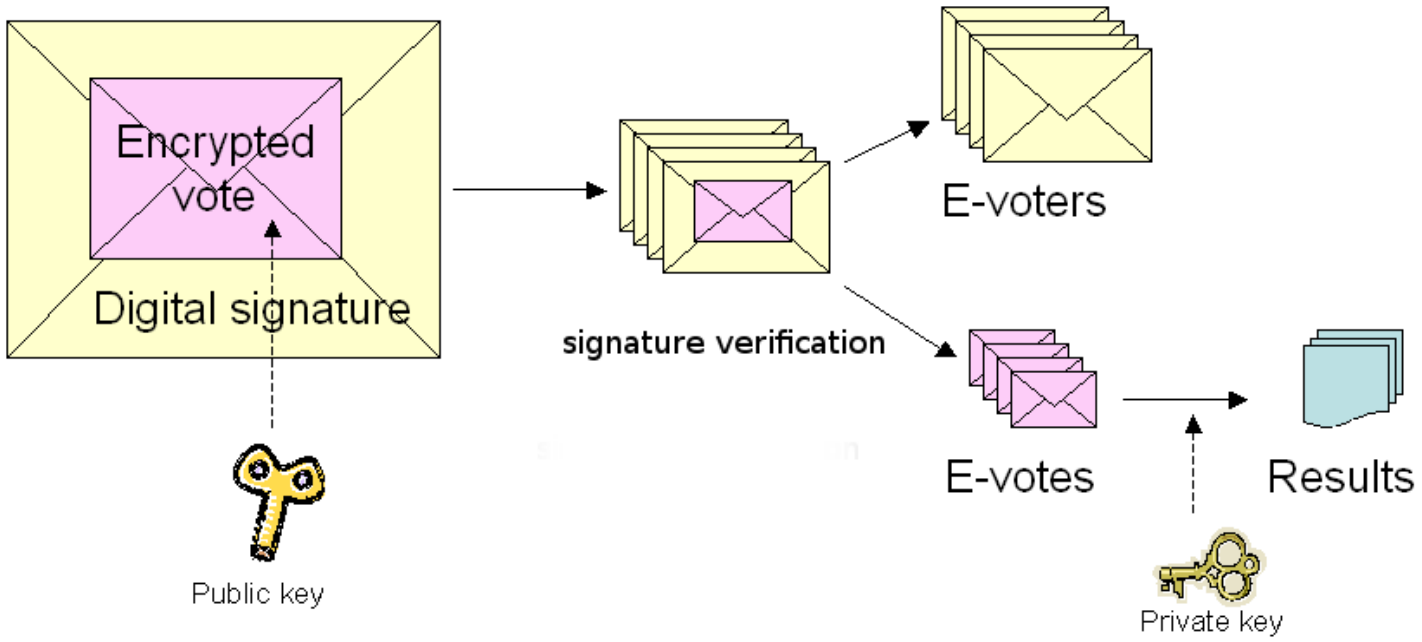
Possibility to export interfaces of a component as Web Service



Authenticity and Anonymity

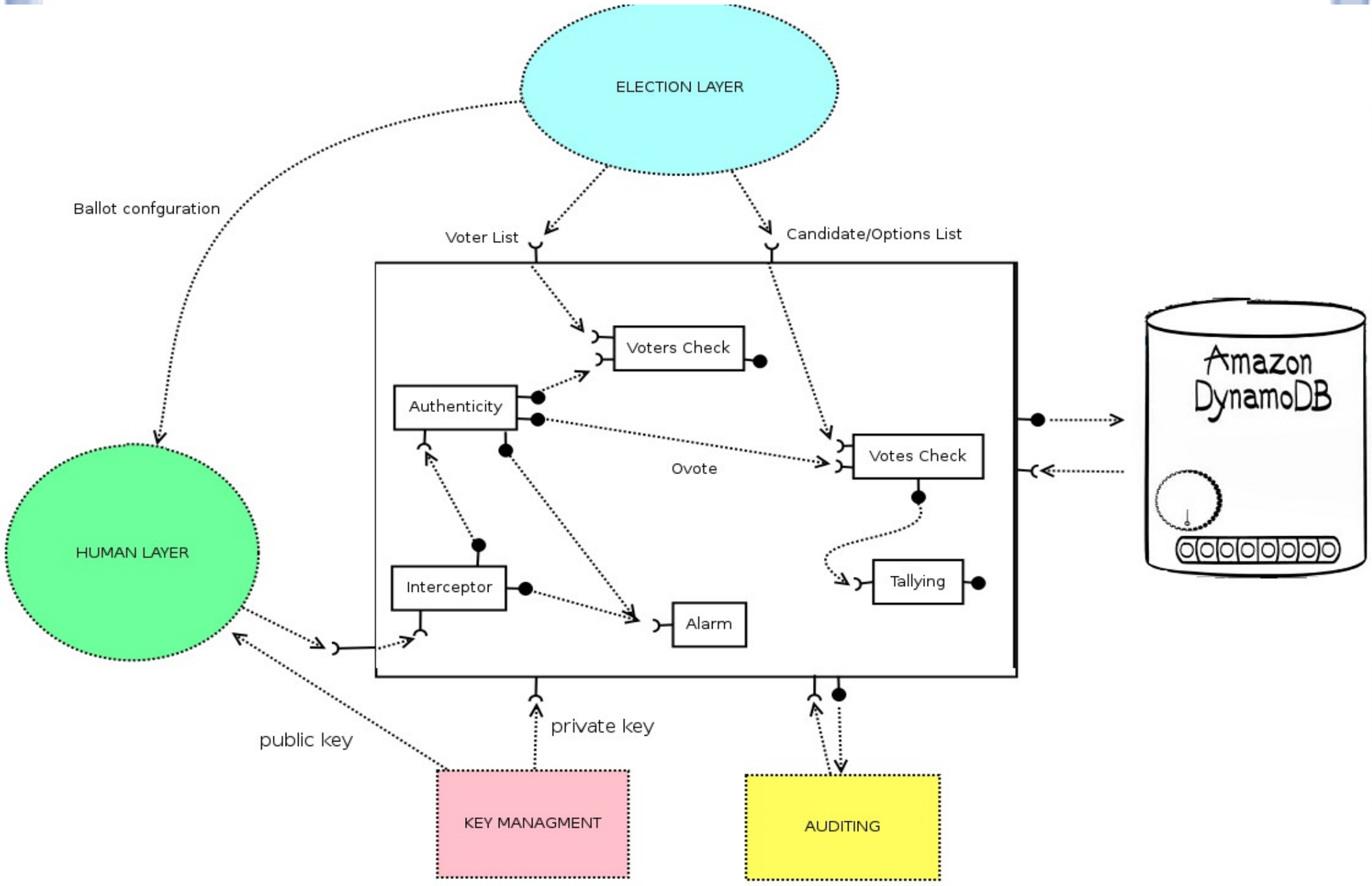
Public Key Encryption and Digital Signatures

- Prevent eavesdropping
- Preserv anonymity
- Authenticity



At no point should any party of the system be in possession of both the digitally signed vote and the private key

A toy example



Conclusions

- Ovote with a component based design
- Easy to verify
- Auditable
- High availability
- Preserves the features of anonymity and unique vote
- Authenticity verification
- Secure communication between component layers