Security functional requirements

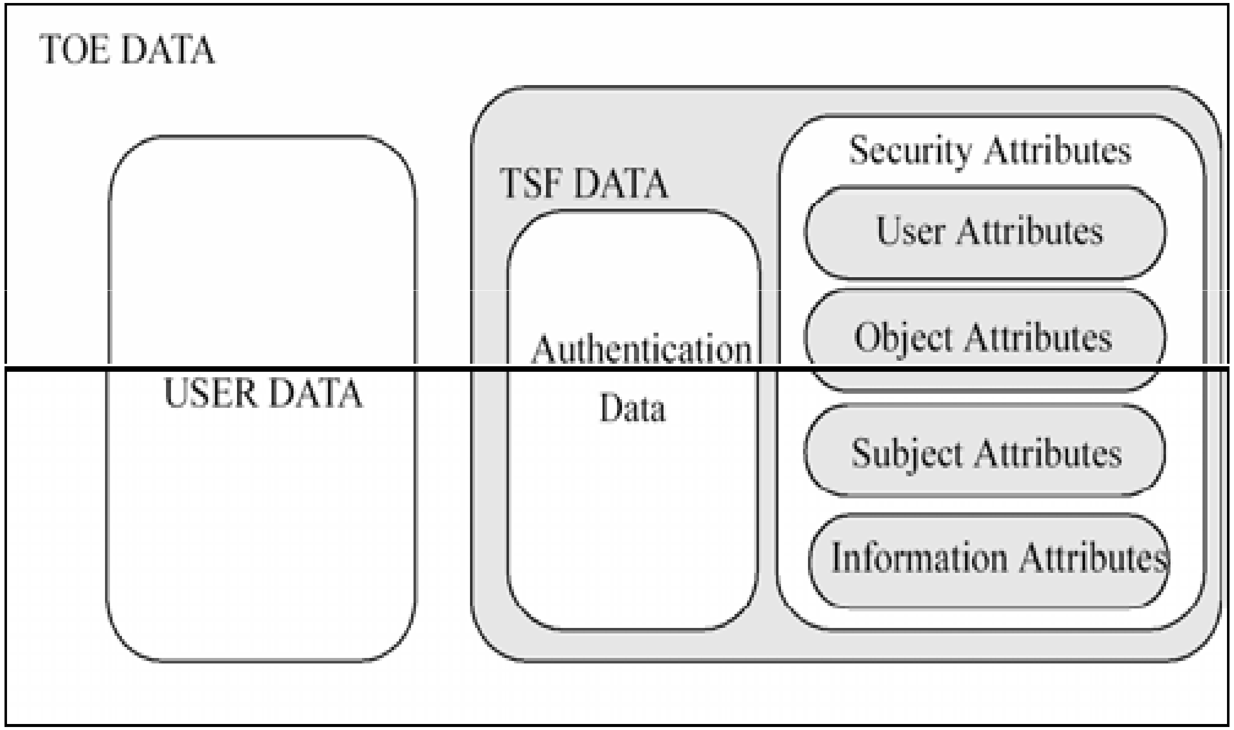
Scope:

Consumers – to select components to express functional security requirements to meet security objectives

Developers – to respond to actual or perceived consumer security requirements

Evaluators – to verify that the functional requirements expressed in a PP or ST satisfy the IT security objectives
- that all dependencies are accounted for and shown to be satisfied

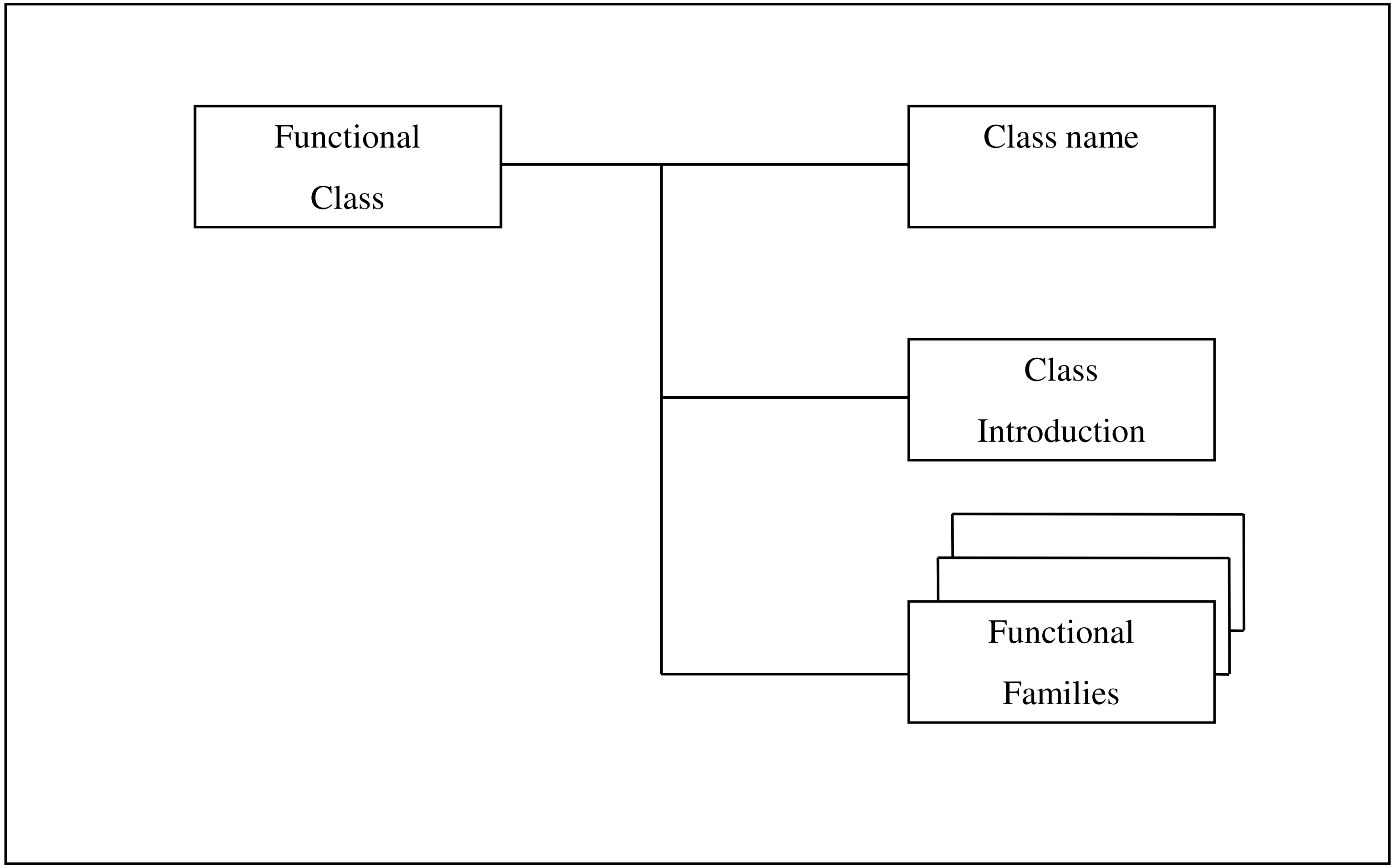
Relationships between user and TSF data and



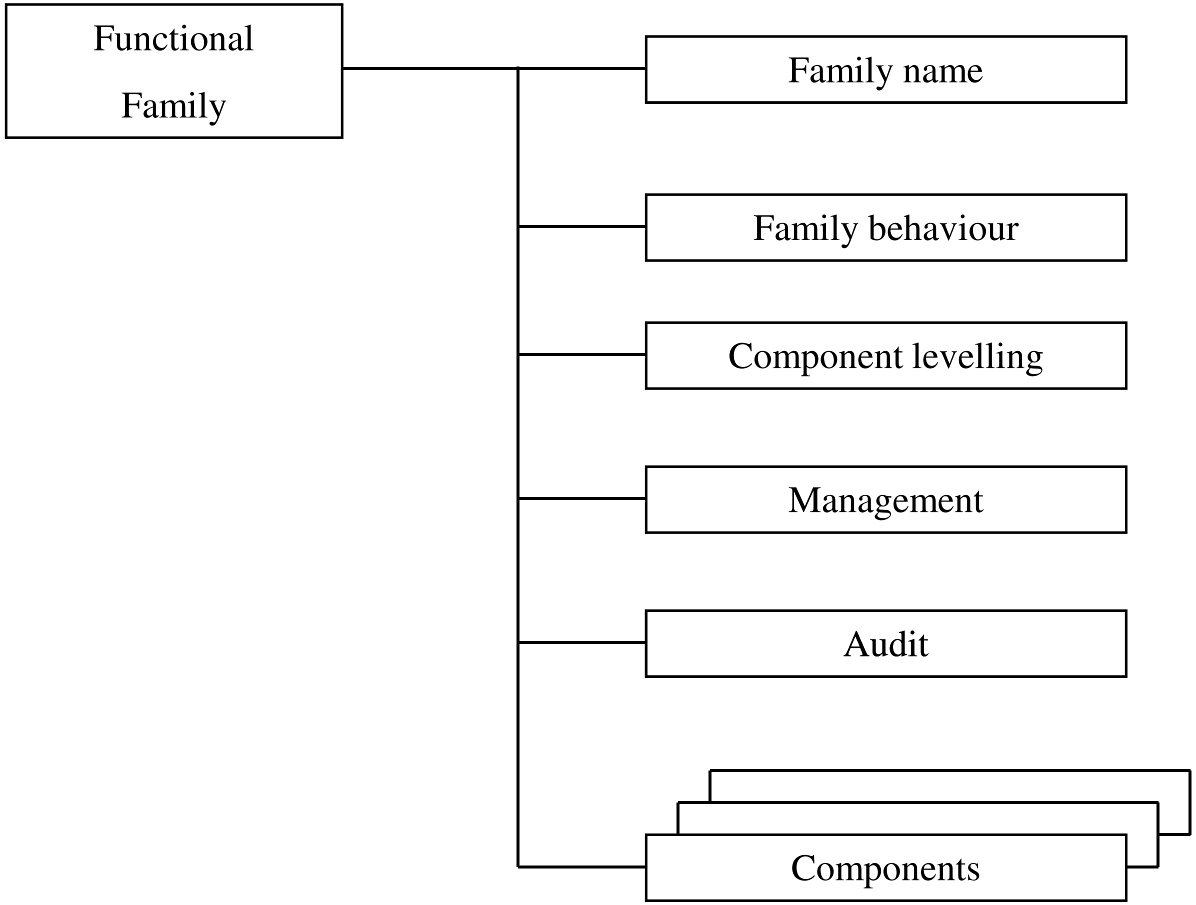
The Functional Class Set

- FAU - Security Audit
- FCO - Communication
- FCS - Cryptographic Support
- FDP - User Data Protection
- FIA - Identification and Authentication
- FMT - Security Management
- FPR - Privacy
- FPT - Protection of the Trusted Security Functions
- FRU - Resource Utilisation
- FTA - TOE Access
- FTP - Trusted Path/Channels

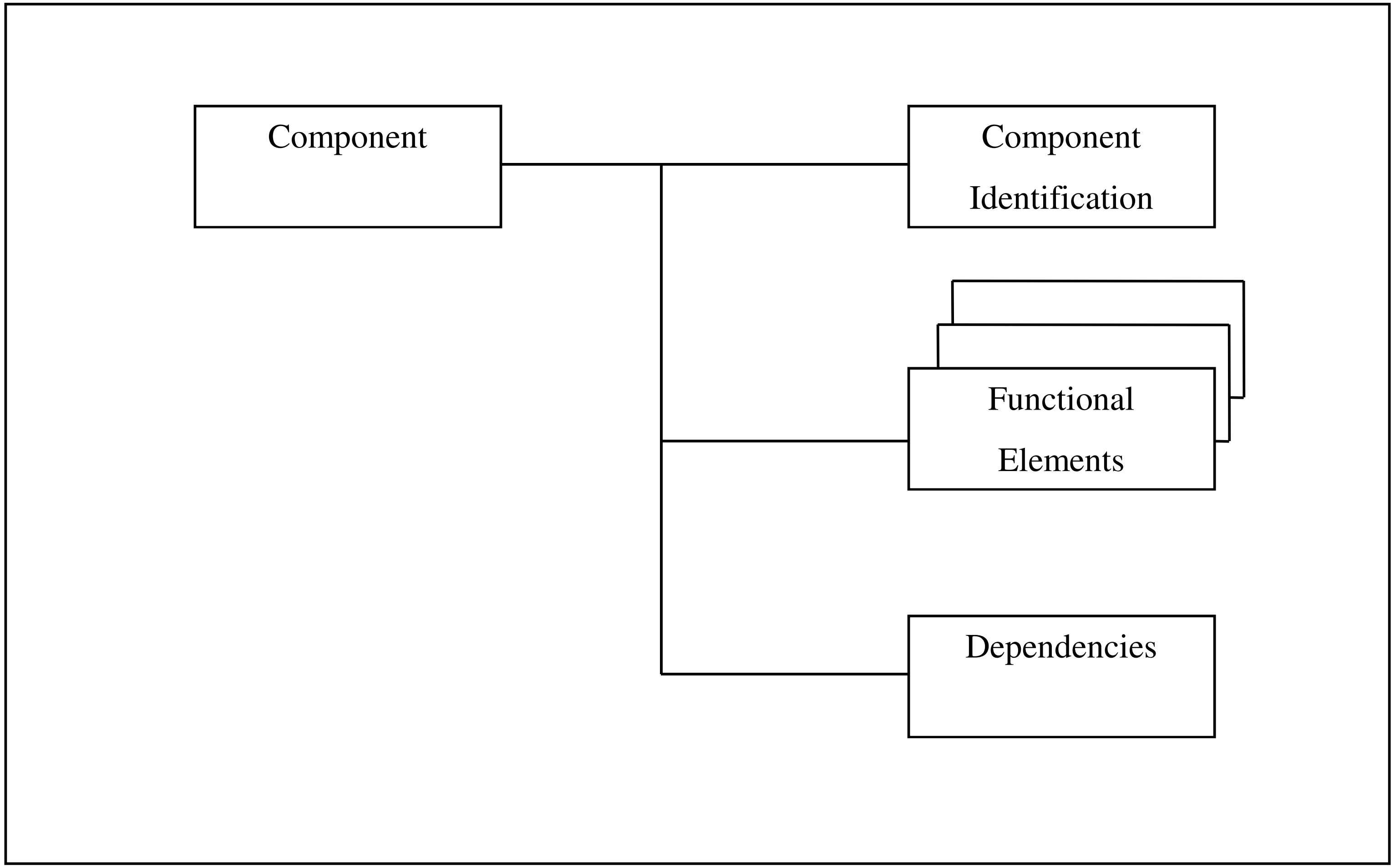
Class structure



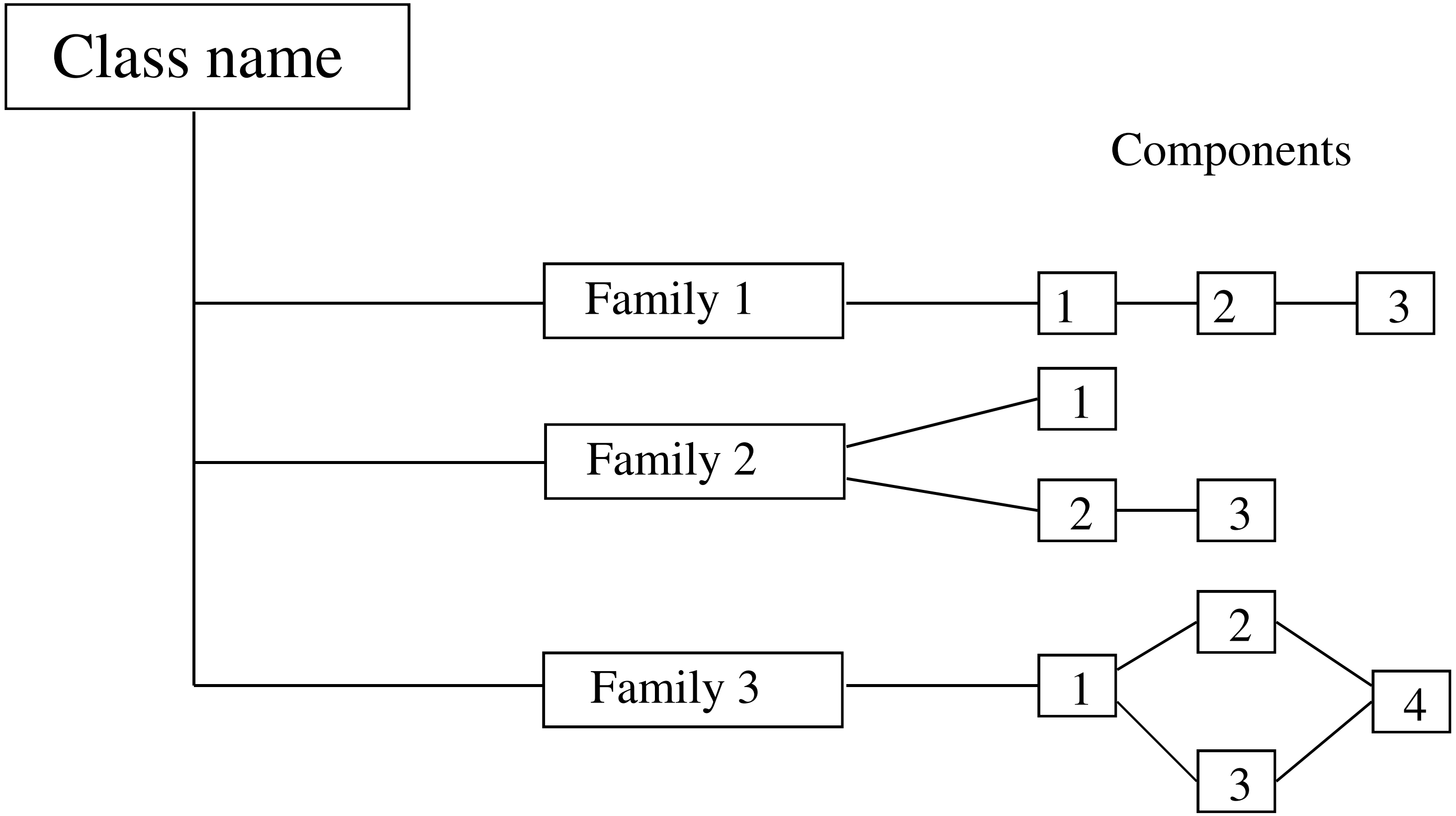
Family structure



Component structure



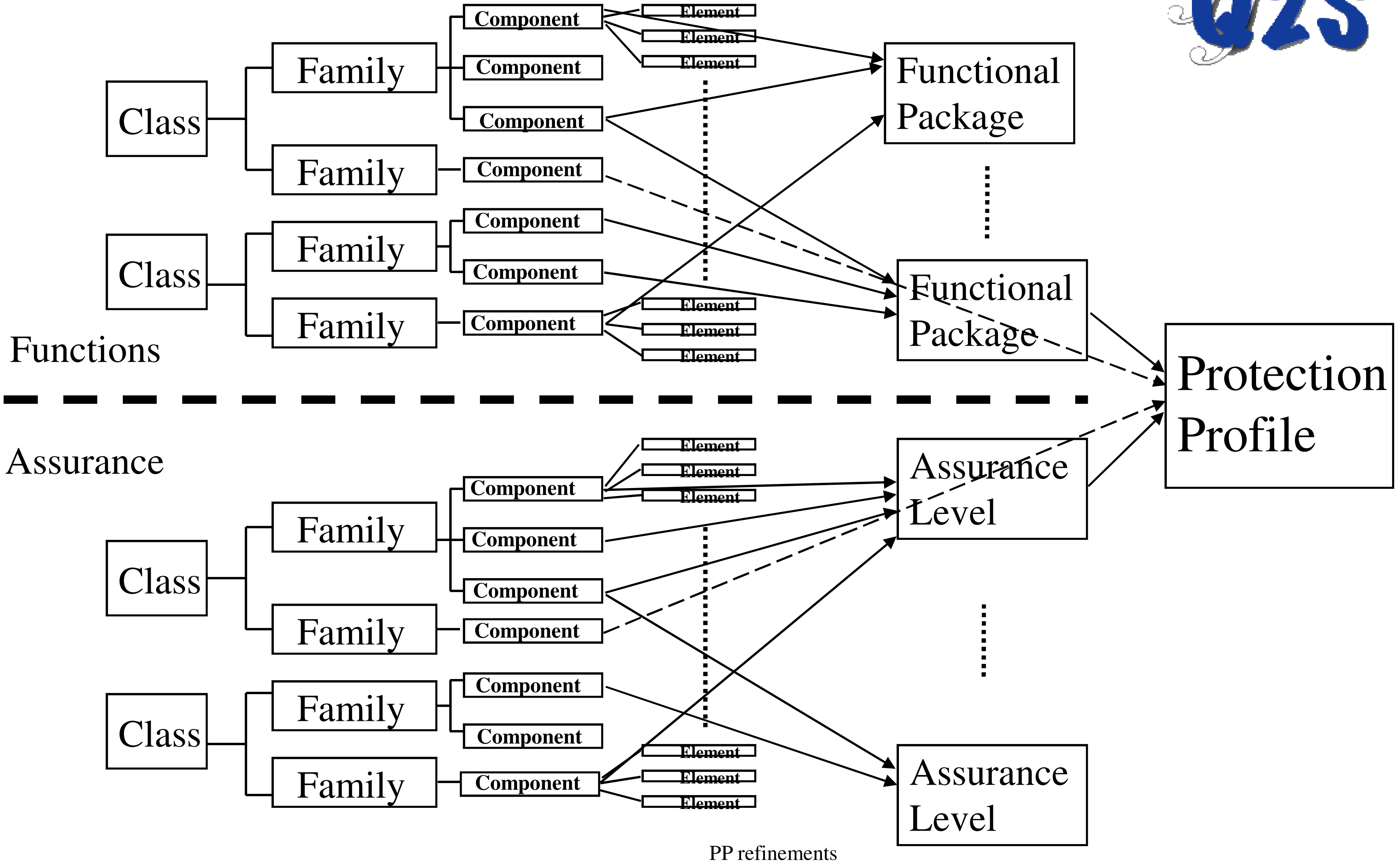
Functional components taxonomy



Component operations

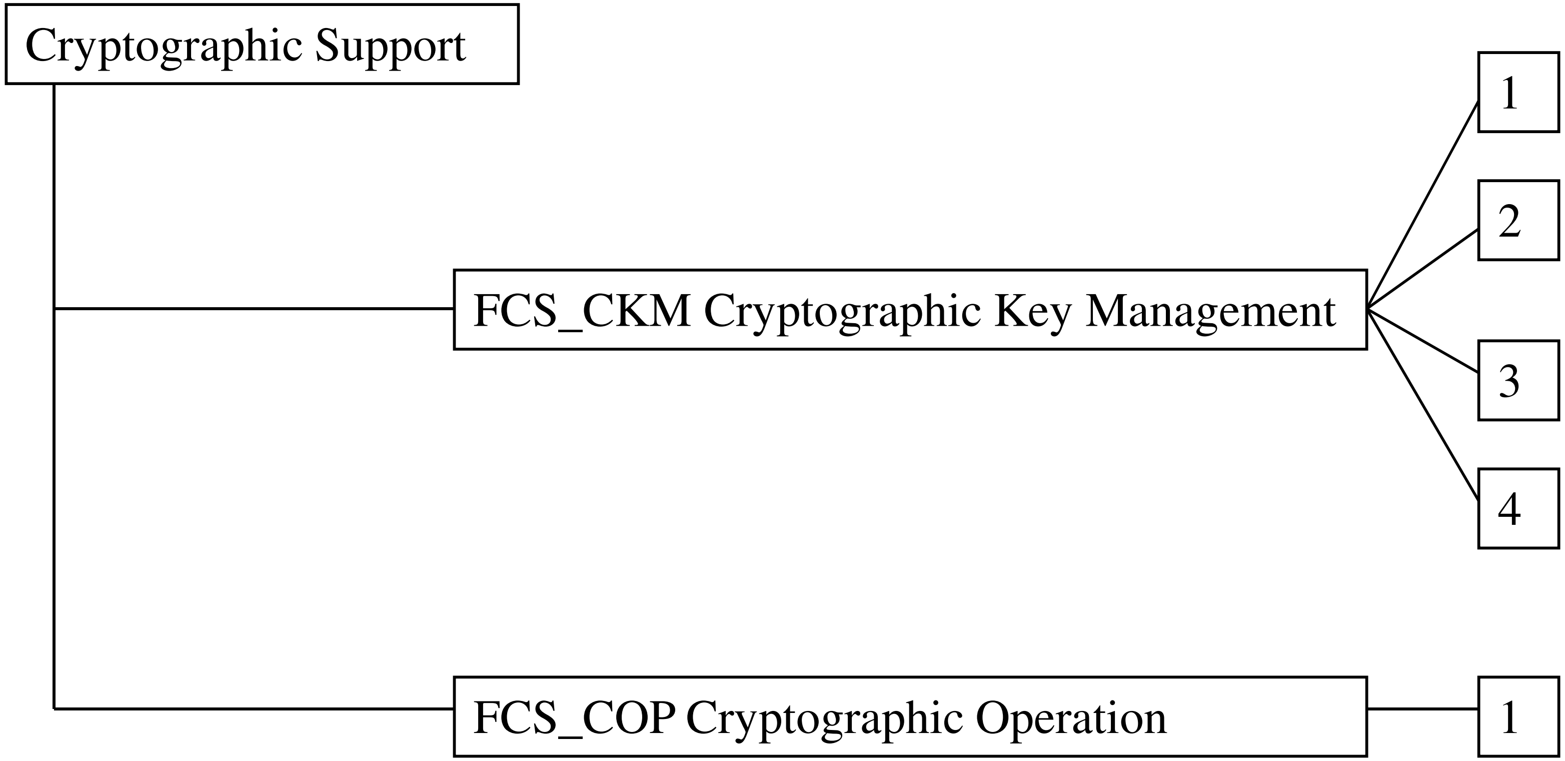
- iteration: allows a component to be used more than once with varying operations
- assignment: allows the specification of an independent parameter
- selection: allows the specification of one or more elements from a list
- refinement: allows the addition of details

The Double Hierarchy



FCS – Cryptographic support

This class is used when the TOE implements cryptographic functions



Cryptographic Support

FCS_CKM Cryptographic Key Management

FCS_COP Cryptographic Operation

Cryptographic Key Management

Key life cycle:

- Generation: In accordance with a specified algorithm and key sizes
- Distribution: In accordance with a specified distribution method
- Access: In accordance with a specified access method
- Destruction: In accordance with aspecified destruction method

Cryptographic Key Operation

- encryption/decryption
- signature generation/verification
- checksum generation/verification
- secure hash generation
- key encryption/decryption
- key agreement

FCS_COP.1.1

The TSF shall perform:
[assignment: ***list of cryptographic operations*****]**
in accordance with a specified cryptographic algorithm:
[assignment: ***cryptographic algorithm*****]**
and cryptographic key sizes:
[assignment: ***cryptographic key sizes*****]**
that meet the following:
[assignment: ***list of standards*****].**