Cuublemesh (Web multi node/multi chain) Platform and Digital Provenance System.

Implementing ZTA (Zero-trust Architecture), with IDM, OSS, PKI in a Service-mesh configuration for online infrastructures, Telco & Cloud Providers

@Alan Lloyd , Director, CIO, Co-founder, Cuublemesh

AKRAINO

cuublemesh

Presentation Topics

- **ZTA The US DOD and NIST Models**
- **The (Web) Systems Front End Issues re Identity, Governance and Systems management**
- **Basic Architecture and Unique Functions**
- **X.500 Global identity Systems – Object oriented identity design methods**
- **Cuublemesh Identity system – operational engineering design approaches**
- **X.509 Global PKI Systems – Object oriented PKI design methods**
- **Cuublemesh Smart Mesh PKI system – operational engineering design approaches**
- **X.700 Systems Management – Object oriented OSS design methods.**
- **Cuublemesh Smart Mesh PKI and OSS – operational engineering design approaches**
- **Systems convergence and the web user interface engineering methods**
- **The cuublemesh platform applications.**
- **Systems transformation – addressing ZTA using platforms, methods and tools .**
- Additional slides FYI e.g.
  - Documents, Signing and Credentials Apps
  - Credentials , Digital Assets, NFTs and Smart PKI/OSS – the Utility

The US Dept of Defence - Zero Trust Architecture

cuublemesh

- https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v1.1(U)_Mar21.pdf
- Department of Defense (DOD) Zero Trust Reference Architecture Version 1.0 February 2021 Prepared by the Joint Defense Information Systems Agency (DISA) and National Security Agency (NSA) Zero Trust Engineering Team

Zero Trust (ZT) is a cybersecurity strategy and framework that ***embeds security throughout the architecture to prevent malicious personas from accessing our most critical assets.***

It provides zones for visibility and information technology (IT) mechanisms positioned throughout the architecture to secure, manage and monitor every *device, user, application, and network* ***transaction occurring at the perimeter and/or within a network enclave.***

Zero Trust is an enterprise consideration and is written from the perspective of cybersecurity.

The foundational tenet of the Zero Trust Model ***is that no actor, system, network, or service operating outside or within the security perimeter is trusted.*** *Instead, we must verify anything and everything attempting to establish access. It is a* ***dramatic paradigm shift in philosophy of how we secure our infrastructure, networks, and data, from verify once at the perimeter*** *to continual verification of each user, device, application, and transaction.*

“a dramatic paradigm shift in philosophy.. from verify once at the perimeter to continual verification of each user, device, application, and transaction.”

An integrated Identity design, its governance, trusted identity verification and the systems management is the key for ZTA effectiveness

cuublemesh

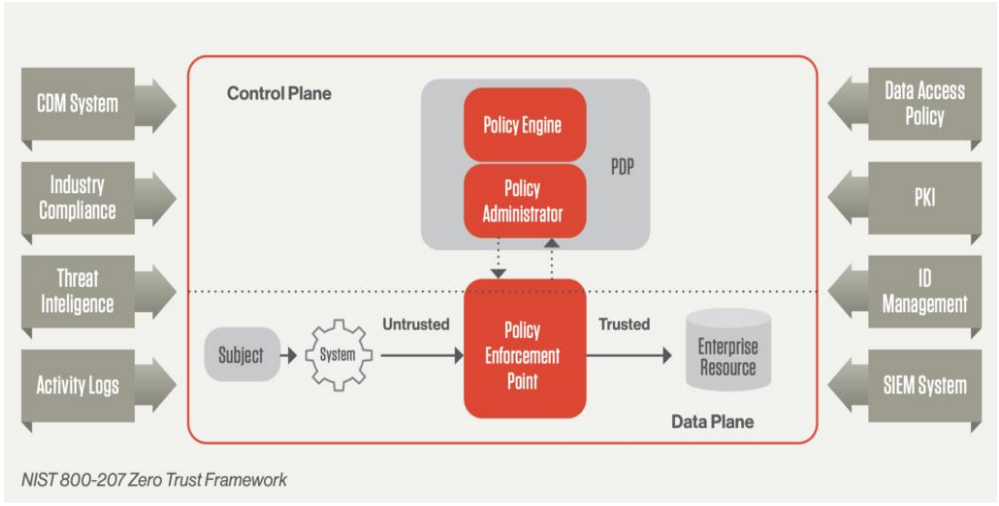
Zero Trust and NIST 800-207

Zero Trust seeks to address the following key principles based on the NIST guidelines:

Continuous verification. Always verify access, all the time, for all resources.

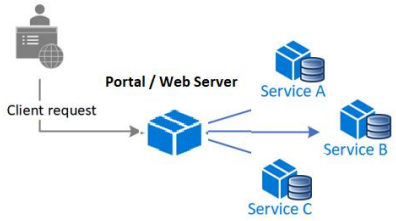
Limit the "blast radius." Minimize impact if an external or insider breach does occur.

Automate context collection and response. Incorporate behavioral data and get context from the entire IT stack (identity, endpoint, workload, etc..) for the most accurate response.



NIST 800-207 Zero Trust Framework

Comment:
ZTA is depicted in a data transactional context



The overall systems information architecture and its identity, governance and systems management and how it is applied is left to the systems architect.

An integrated Identity design, its governance, trusted identity verification and the systems management is the key for ZTA effectiveness

cuublemesh

The US Dept of Defence - Zero Trust Architecture

Client and Identity Assurance - Person and Non Person

Authentication and Authorization. - with policy enforcement points

Data Centric Enterprise. - Resources, Application, Data, with policy enforcement points

Policy Enforcement Engine. – enforcement, analysis and collection.

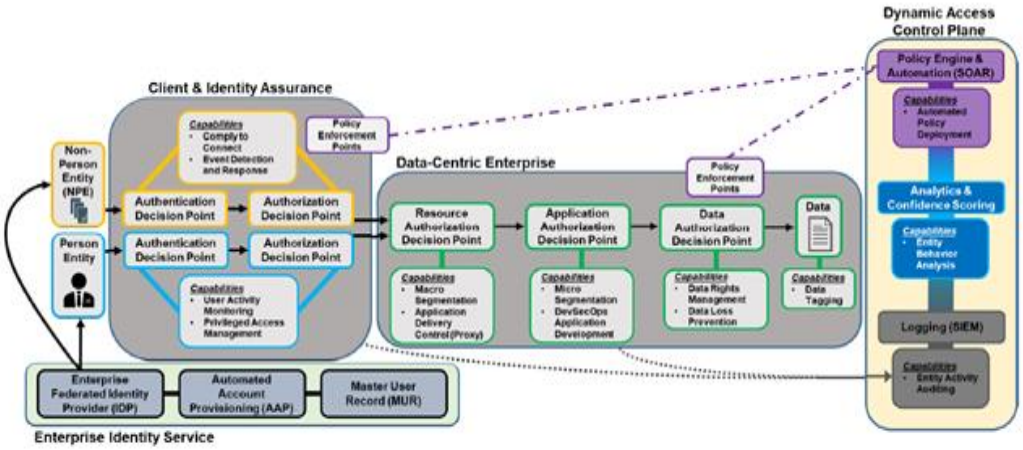
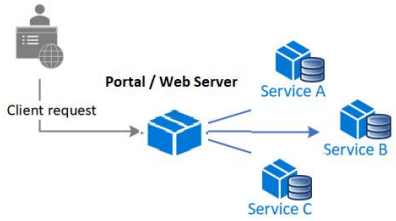


Figure 2: High-Level Operational Concept (OV-1)

Comment:
ZTA is depicted in a data transactional context



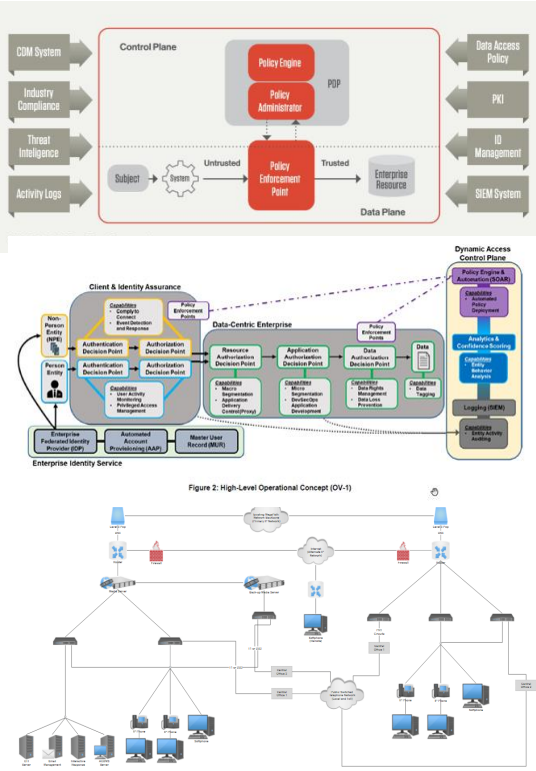
The overall systems information architecture and its identity, governance and systems management and how it is applied is left to the systems architect.

An integrated Identity design, its governance, trusted identity verification and the systems operational management is the key for ZTA effectiveness

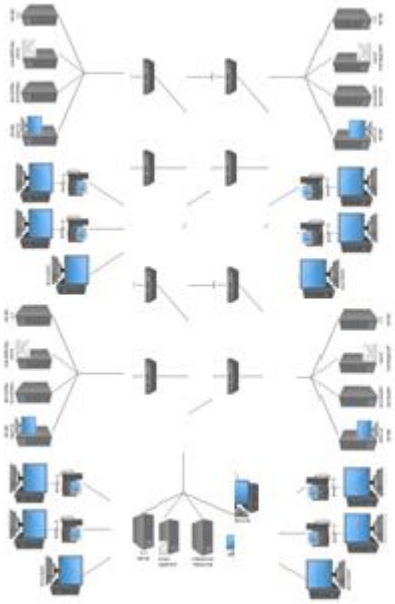
cuublemesh

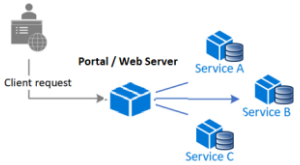
ZTA– what are the complications and a way forward

Models and Technology Architectures



Scaled up Technology Architectures, are they too complicated?





The labels of the ingredients

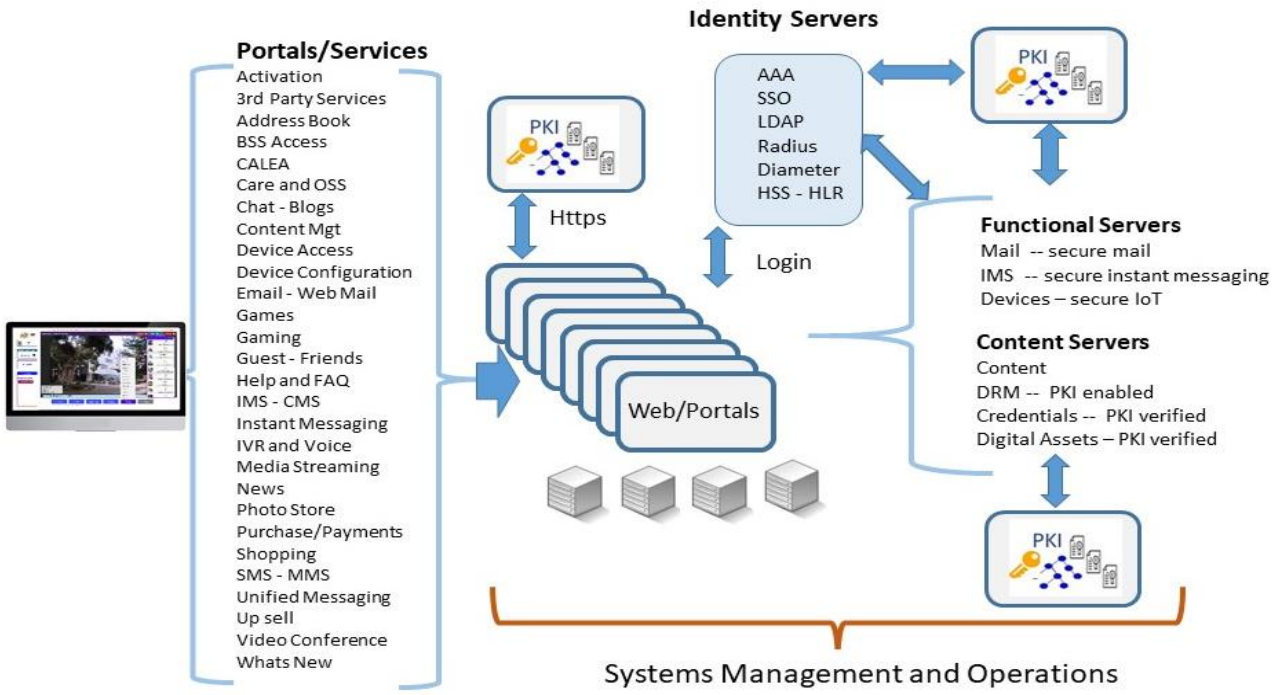
Identity
Access Controls
Governance
Validation – PKI
Network Addresses
Systems Management
Security
Portals
Servers
Applications
Databases
Content
Work Flows
Digital Assets
Users

The system's information architecture, its identity, governance and the dev ops systems management dimensions … are not defined here.

Putting labels on the system's 'ingredients' and what they are and do in the operational (information) system, how they use identity and governance information and are controlled - managed … is the first step in addressing ZTA.

cuublemesh

A web system front end - a reality example:
A Telco / MSO customer facing system's portals and servers

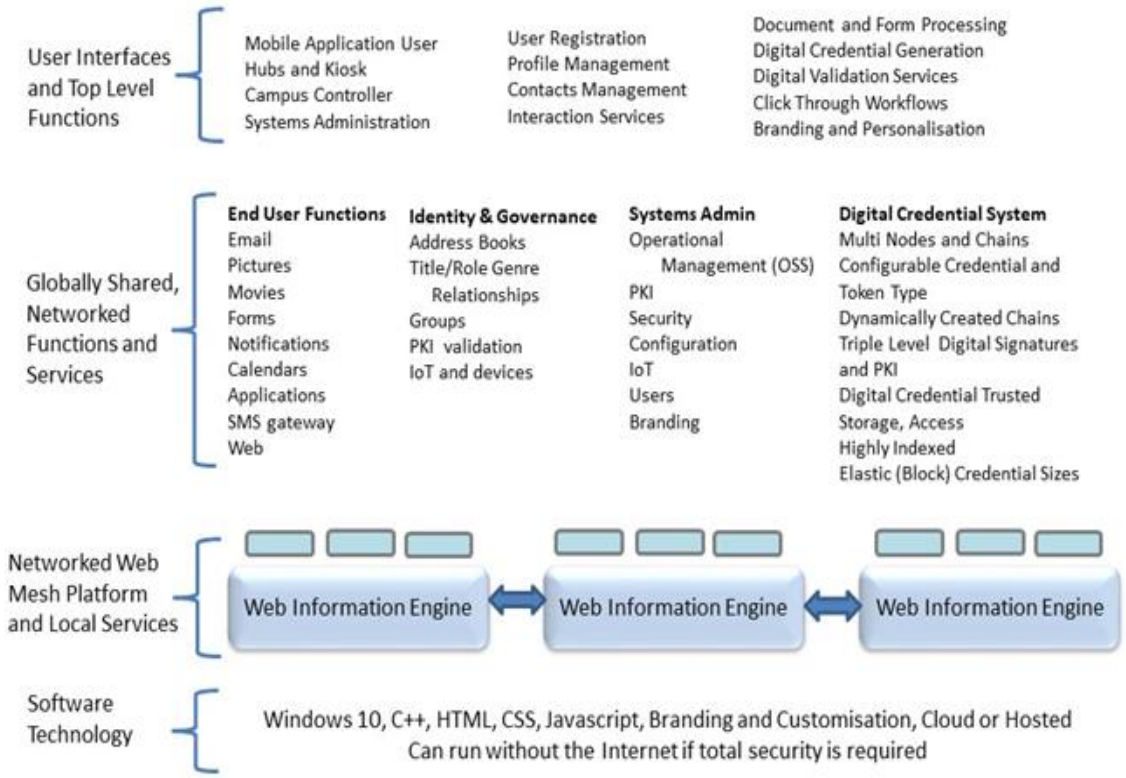


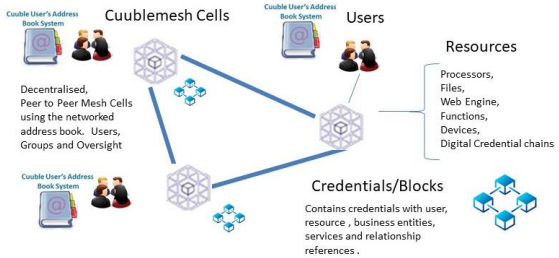
30 – 200 web and identity enabled servers possibly, with IT designs from Internet 1.0 and well known server interfaces and software strengths and weaknesses – and some with technology centric command line based systems management .

Identity Information – everything in the system has it and uses it.

This situation indicates the need for a new approach to "front end server(s)" design. e.g. a mesh web engine, a platform with integrated core system functions – identity, governance, validation-PKI and systems management – and supports user services and applications, including using 5G services.

The cuublemesh functions/modules





Unique Features

- Meshed Web Engine
- Soft Configured Role-Class Mesh Wide Identity Management System
- Multi Node, Multi Chain, Elastic Block Size, PKI Enabled Digital Credential and Digital Asset System
- Smart Mesh PKI for User and Digital Asset Creation and Management
- Integrated Systems Management Operational Support System (OSS)

The diagram: a mesh web engine functional architecture, a new breed of web platform with integrated system functions – identity, governance, validation-PKI and systems management – and end user services and applications.
Being web – its focused on user self management, click through workflow, accessibility, human interactions and digital asset trust.

Lets see how it applied the ISO/ITU standards of X.500, X.509 PKI , X.700 systems management, Defence PKI/security standards, web **information systems design** and **Object Oriented engineering methodologies**.

cuublemesh

The (White Pages) Directory (ITU X.500),
The biggest, distributed identity ledger in the world.

The ISO/ITU X.500, X.509 and X.700 are an abstract object oriented (OO) distributed information systems – engineering methodology – for identity, governance, trust and systems management.

Please Note: These standards DO NOT prescribe the technology implementation.

White pages identity information exists all over the world in files, web pages, telephone books, documents, forms, contracts, phones, PCs, billing systems, labels, bill boards, vans and trucks, news and media, search engines and on works of art, etc . And we are all asked to keep records for years with such identity information.

Our nations , jurisdictions and law, governments, health, economics, society, transport systems, mapping - location and navigation services – all depend on its design, its attribute sets and its global management.

*At this point in time in this presentation **it is critical not to consider any form of IT data technology, mechanisms or products here**. This part of the presentation is about global, corporate and **trusted information systems engineering methodologies using our ISO/ITU X. series standards** - as used globally on large scale ICT system infrastructures over the decades.*

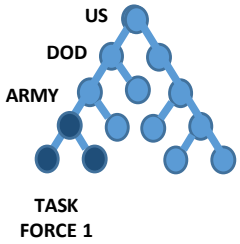
cuublemesh

Identity and Governance Engineering - X.500. The Directory.

- Our world operates on identified entities: e.g. nations, organisations, states, locations, users, devices.
- And we represent these real world identified and governed entities in a global directory (our white pages) as information objects. All objects in the 'directory' have a class (e.g. country, organization, etc) and a name (e.g. US-DOD). Their name is the object's identity,
- Identity and **identified objects as per real life are usually placed in a hierarchy thus a governance structure is assumed**. E.g. US, DOD, ARMY, TASK FORCE 1
- i.e. The US entity governs DOD, DOD governs ARMY, ARMY governs TASKFORCE 1, TASK FORCE 1 governs its members.
- Our postal and telco systems are global functions that route physical packages or telephone calls using such 'white pages' directory information. The internet routes data packets on domain names and IP addresses. Its directory service is DNS . Domain names and email addresses form part of the white pages .
- The ISO/ITU information systems standards for our global white pages , the worlds biggest distributed, identity system design is specified in x.500. It is a set of standards which define the design elements of the worlds operational identity system which underpins the way the whole world interoperates, our governments and laws are bounded, how are maps are produced, etc.
- The x.500 standards were produced in the late 80s by our international standards bodies – the ITU and ISO to address telco, postal, internet directory systems, identity and distributed information systems engineering. **They have been applied globally in most systems today – one way or the other.**

ISO/ITU X.500
Directory
Identity Hierarchy

A Directory Example



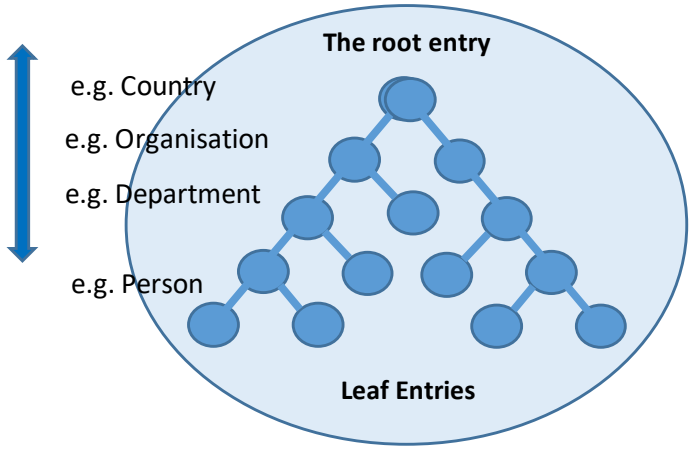
ZTA - identity, validation and systems management. The "Friend of Foe " question.

cuublemesh

The Directory Name Space: – a collection of identified objects, - using object oriented systems engineering

A Hierarchical Name Space of objects where each must have a class and an identity attribute – with a unique identity value.

A Name Space



In reality our global white pages directory system works in this hierarchical way. Countries at the top.. states, cities, localities, organisations, applications, devices and residents at the bottom.

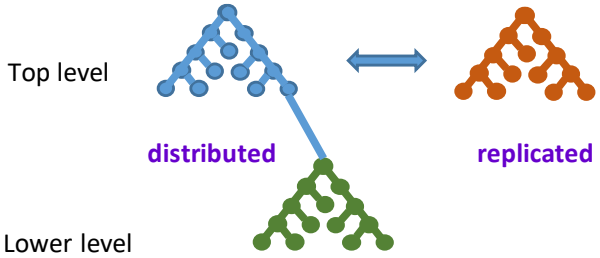
Our Governments, Legal, Postal and Telco systems, etc.. Basically all of us rely on this global white pages identity systems design, standards, structure and its information.

- We have OO software languages and standards - C++, HTML, JS, JSON JQUERY, even CSS (web page style sheet specifications are OO) , x.500, x.509, x.700 – systems management, - managed objects.

- **It follows that to software engineer a system one must have determined the identity and the governance regimes and how these objects/information sets (as in real life) are used, interrelate, interoperate and are managed…**

ZTA actually demands this…

Replicated and Distributed Name Space



Name spaces (of identified information objects) can be **distributed** or **replicated** as per the telco white pages .

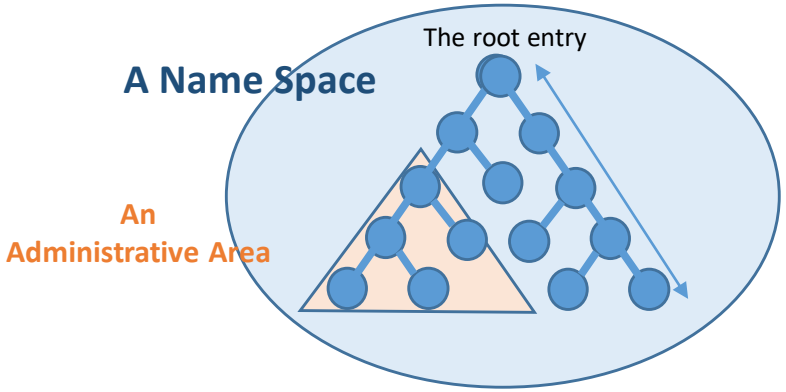
X.500/501 covers the following topics:

cuublemesh

A Name Space(s) are an area of named/identified objects under governance – a governance area is called an Administrative Area

X.500/501 topics cover:

- Distributed Directory System Models
- Name Space design
- Administrative Areas – Name Space Governance
- Access Controls on the Name Space
- Directory Schema – Object Classes, Attributes
- Naming (identity) methods
- Name Bindings and Name Containment
- Knowledge of Name Space
- Navigation through Name Space
- Interconnection of Distributed Name Space
- Interconnection of Replicated Name Space



If one is designing a (distributed) information system in software one uses OO methods to define every information set within the system that represents a resource of the system with its identity – and the interactions it has with other objects – identified entities..

The subject matter list (left) provides distributed information systems engineering subject areas, methodologies and guidance in this regard.

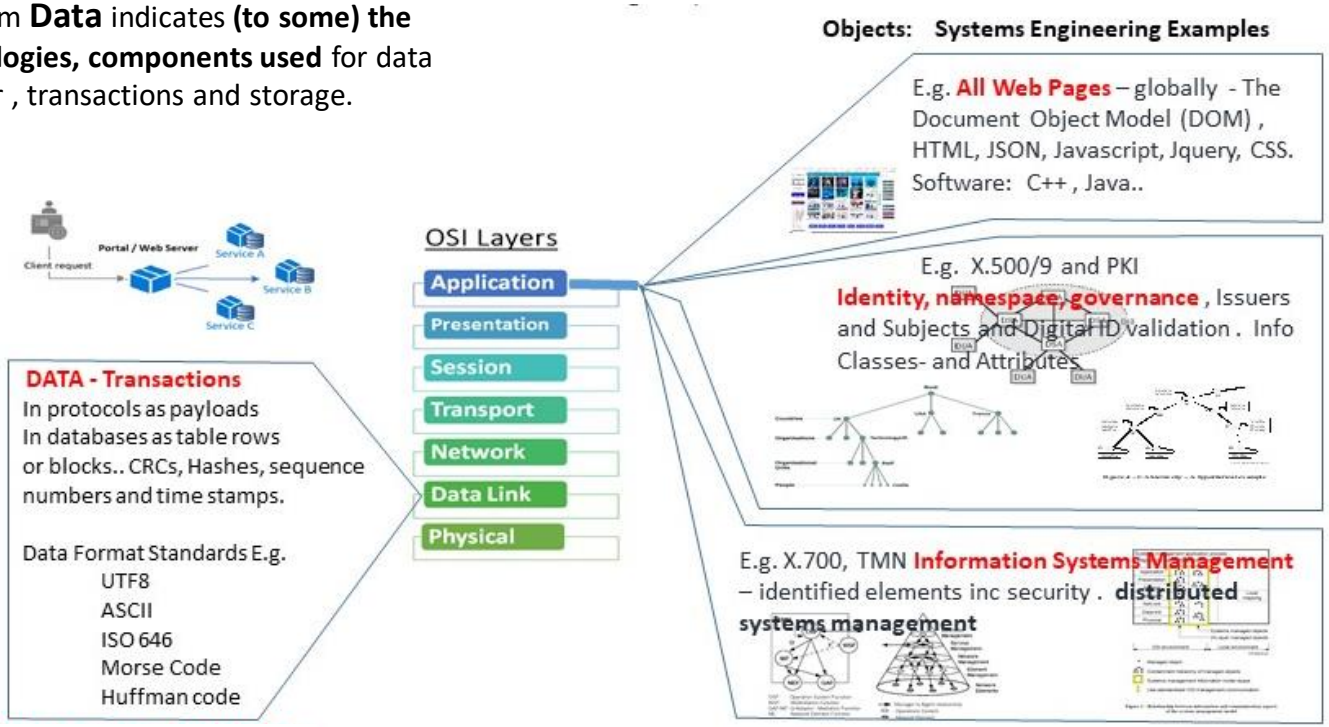
ZTA - identity, validation and systems management.
The "Friend of Foe " question is always asked in a context and a namespace.

cuublemesh

Data and Information – distributed systems engineering… The difference.

In online systems design and standards:
The term **Data** indicates **(to some) the technologies, components used** for data transfer , transactions and storage.

Information on the other hand, indicates **(to some) what we as humans use, understand, manage and trust** (the language of) the (distributed information) system , **regardless of the nature of data technologies**, transactions and networking components used.



To the left of the OSI diagram, with the system design, its identity, validation and systems management engineering *methods are not visible*, to the right we have global standards for both web technologies and managed, trusted information infrastructures.

System Design Basics : Transactions and Data – Information, Users and Scale

Scale is based on the technology used.
Transactions Per Second

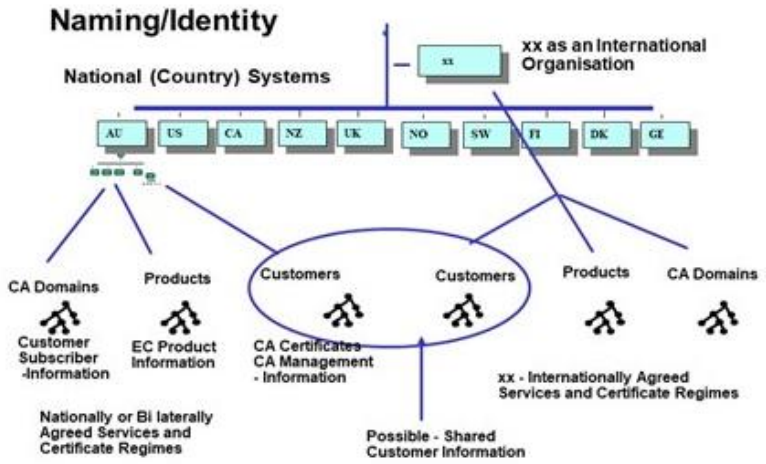
The OSI reference model
– courtesy (late) Jack Houldsworth ICL late 1970s, "the grandfather of OSI"

OSI - A framework for the standards for distributed information systems

ISO/ITU X.200

Scale with distributed information systems and identity (OO) engineering is about **interconnected namespaces (nodes) where each namespace can have delegated (decentralized) governance.**

Scale is based on the information - Identity, governance and systems management design.



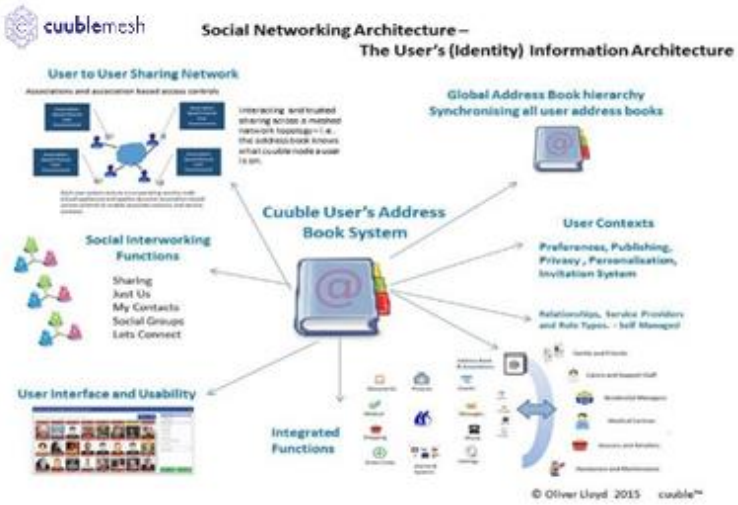
Directory diagram from mid 90s

Global infrastructures are designed around identity – interconnected names spaces and their governance. They scale that way.
We underpin these designs with networks, processes and data storage methods that suit the operational use of the namespace.

Cuublemesh Identity (Address Book Namespace) System Design

The cuublemesh address book provides the identity and access interaction core of the mesh.
– initially designed 2015. It's a networked, configurable relationship-Interaction-identity and access system

- 3 Levels – 1. Mesh, 2. Node and 3. Organisation, Service, User, Device, Livestock
- IoT addressable, email and personal web sites
- Software configurable Role, Title, Class and Genre Hierarchy (e.g. Family, Health, Education, Finance, Food Supply, Devices)
- Designed on how one personally labels, trusts and finds things easily and what one interacts with.
- Has publishing and privacy controls – profiles and groups.
- Variant attribute sets provided for Users, Devices, Credential Chains, Organisations, Services, 5G devices , Livestock.
- Has functional variants for specific roles: Administrator, Operators, Users , Social Groups, IoT Devices
- Identity and PKI information is propagated across the mesh according privacy controls and system services.
- Supports the intra node and mesh messaging, notifications and content transfer system.



Identifiers and their system levels - *i.e. Information at the Global, Nodal and Personal Layers need management*

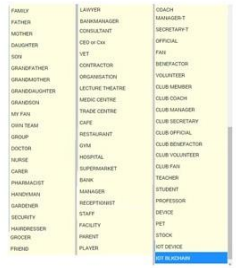
Cuuble Mesh Nodes

Attribute Numbers = (N)

- **Mesh** – Global System Level.. (nodes, address book, groups, credential chains, devices)
- **Node** – Local Level.. (node, address book, groups, credential chains, devices)
- **User** - Personal Level... (user profile, address book, user groups, credential chains, devices)
- **IoT Device** – Device Level... (identifiers and configuration)
- **Messages, Events , Credential Types, and Smart Contracts**.. (identifiers and content)

Address Book Entry (User entries * 70) for people, IoT devices inc BC, pets, services
Credtl Chain Config (N Chains * 30)
Credtl Types (25 * 25 avg)
Smart Contracts (N * 40)

Address Book - Role, Title, Relationships
Soft Configured – Class and Genre Hierarchy



Per User/Service Profile

Contact details (15)
Preferences and Privacy (12)
Password management (10)
Campus (10)
Licence and Branding (9)
Visual Accessibility (7)
Audio Accessibility (8)
Profile Extension (6)
Help Call ctrls (7)
IoT Dev ctrls (N * 3)
Email Account ctrls (5 * 18)
Block Chain ctrls (8 * 3)

200+ profile attributes per user

Plus Per User Info Items
Mail Boxes, Notifications, Personal Web Site Pages, Picture Gallery, Documents, Scripts, Logs, etc

The UX – Users require and rely on so many ways of identifying and relating things

Having the system's identity and governance functions as the core - ZTA can be applied coherently and effectively

cuublemesh

Policy Based Access Control Systems – Part of Identity Design

Multi-Service Operator (MSO Service Delivery Platform (SDP) and Policy Based Access Control (PBAC)

Alan Lloyd - August 2011 https://cuublecloud.com/papers/SDPSandPBAC.pdf

"The paper recommends the use of information and identity engineering doctrines with a focus on governance methodologies and service management functions." The paper also identifies with use/device session control functions.

Access Control Contexts:

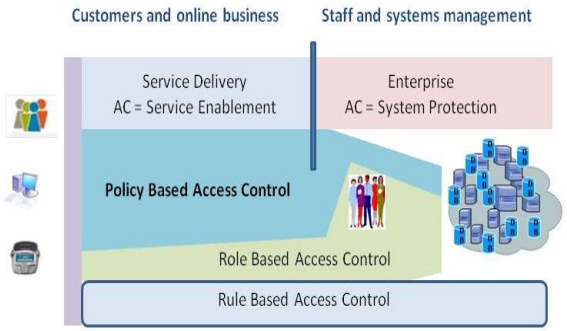
Rule based Access Controls – A rule, the determination of a processing path based on input conditions and

Role Based Access Control - The responsibility assigned to something instantiates their Role, which is then used, governed and tested by other Role based agents (the group).

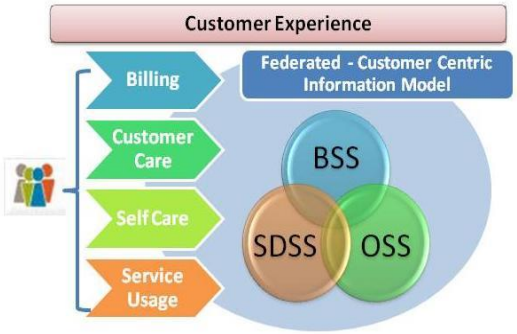
Policy Based Access Controls Allow for the expansion of AC methods into many areas of IT system application be they static or dynamic, for security management or for customer facing functions.

Profiled Session Controls – Landing Pages Allow for the accessor by Id , Role / Title to access particular web pages and work flows. The session access context can be for Administrators, Operators, People, Groups, Application Specific needs or Devices.

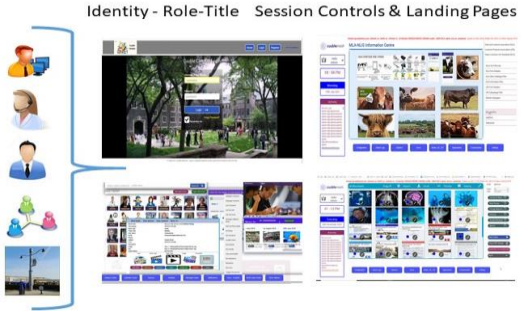
Access Controls



Implementing PBAC &Touch Points



Profiled Session Access



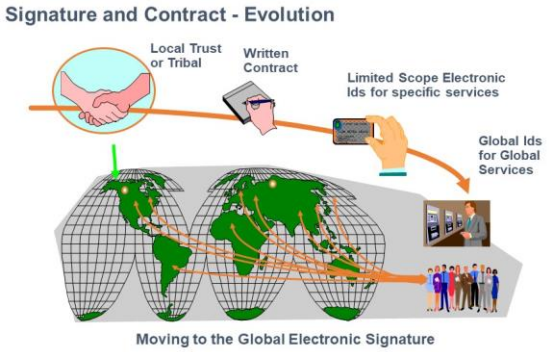
Access Control regimes for identity systems are defined in X.501 and X.509. Session control systems need dynamic within session identity keys – like frequency agile radio channels. Channeled user centric touch points with partitioned environments provide - Separation of Duty as per Multi Level Secure Systems –keeps the attack surfaces and any 'blast radius' small

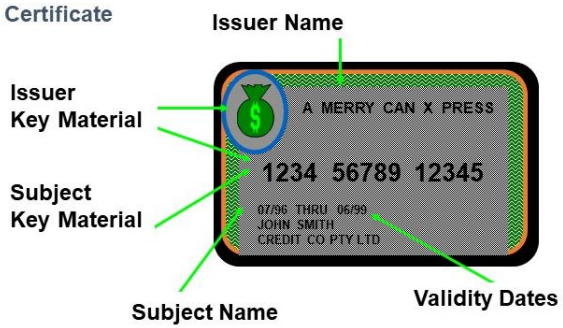
X.509 PKI and Certificate Authorities, Legally Verifiable Identity Based Trust Anchors

X.509 THE DIRECTORY: AUTHENTICATION FRAMEWORK

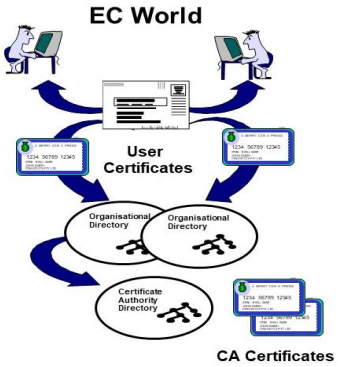
X.509 1997 SECTION 3 – STRONG AUTHENTICATION….. S7 Basis of strong authentication

The approach to strong authentication taken in this Directory Specification makes use of the properties of a family of cryptographic systems, known as public-key cryptosystems (PKCS). These cryptosystems, also described as asymmetric, involve a pair of keys, one private and one public, rather than a single key as in conventional cryptographic systems.





Certificate Authorities (PKI)
Identity based trust hierarchies.
(Chains of trust)



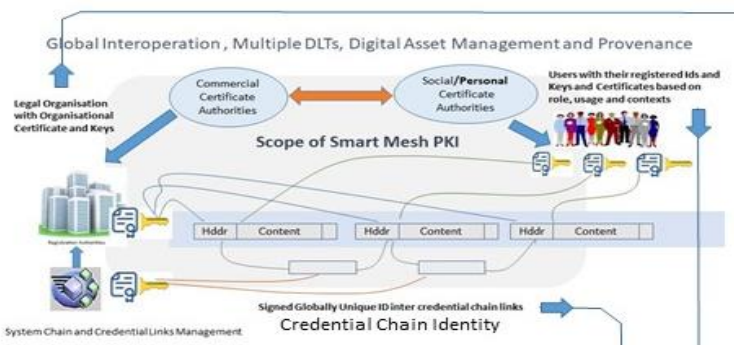
Slide content from 1996

Cuublemesh uses X.509 – Defence standards style 'Attribute Certificates' as its triple level, digitally signed chained credential blocks…. And uses an integrated smart mesh PKI/OSS to manage these credentials as legally verifiable, proof of provenance – digital assets.

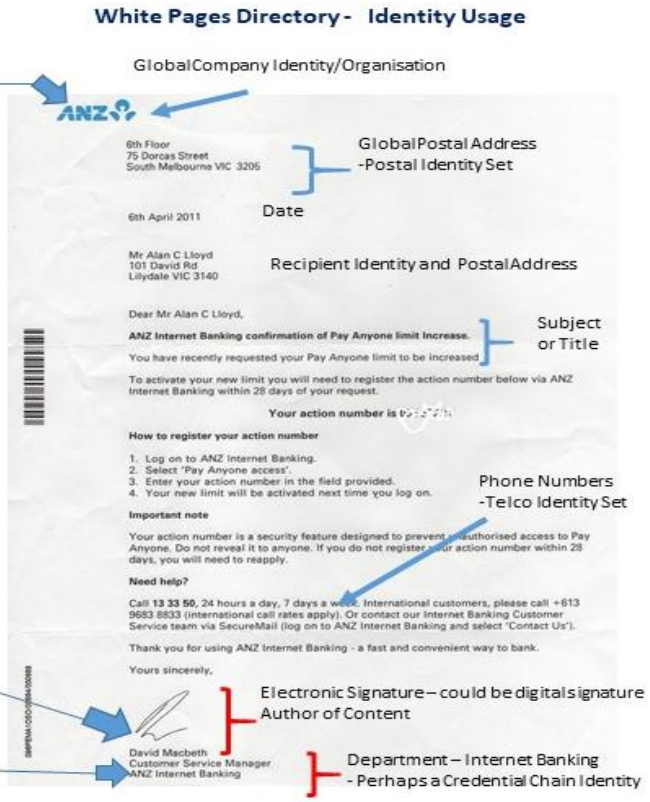
Relating digital assets to paper based and digital identity systems and PKI

Relating the cuublemesh triple digitally signed X.509 Attribute Certificates / Credential Blocks to the worlds legally verifiable global identity system – White Pages (X.500/X.509 PKI) Attributes and trust anchors.

cuublemesh Digital Credentials have elastic block sizes to accommodate user's content, that being one or more documents, images, voice, videos .



- Three Levels of Identity and Digital Signatures
- Multi Node, Multi Chain
- Dynamically Created Named Chains
- Smart Mesh PKI integrated with OSS
- Integrated PKI and Chain functions used to manage Digital Assets and Credentials within and across Organisations, Chains and Authors



Three levels of digital signatures

Organisation

The Chain Id (department)

Author or Device

ZTA - identity, validation and systems management.

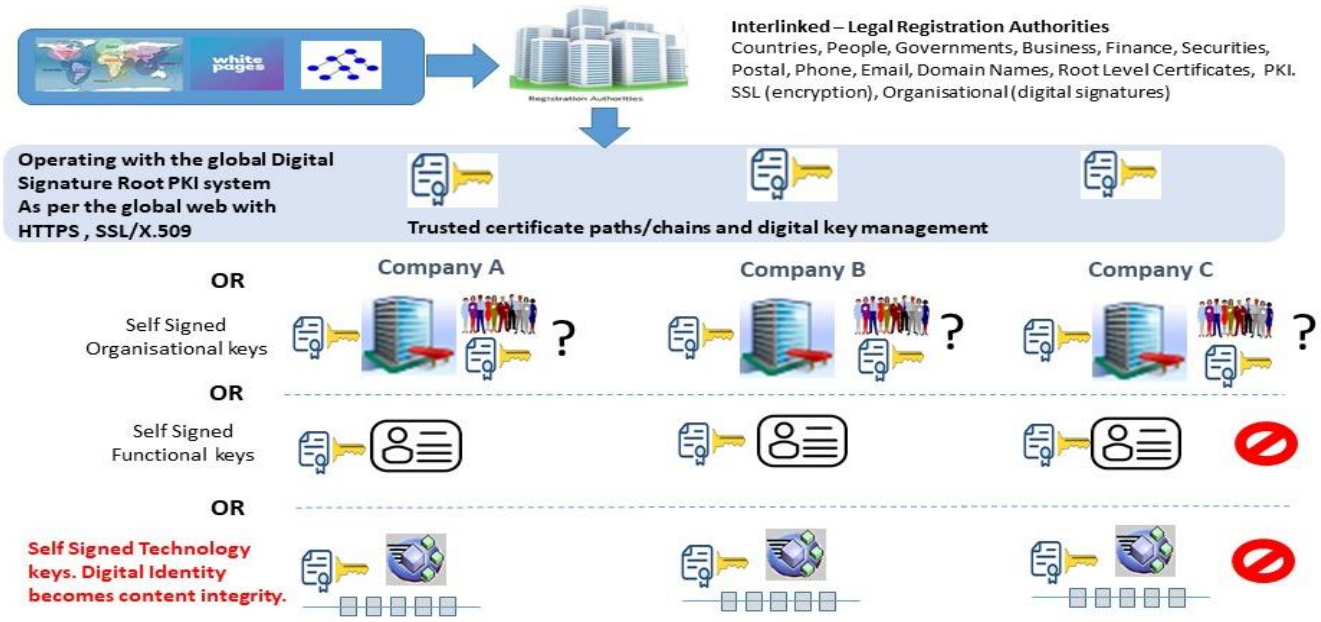
Validation systems and their management – essential for PKI and ZTA

cuublemesh

PKI - Legally verifiable identity trust anchors

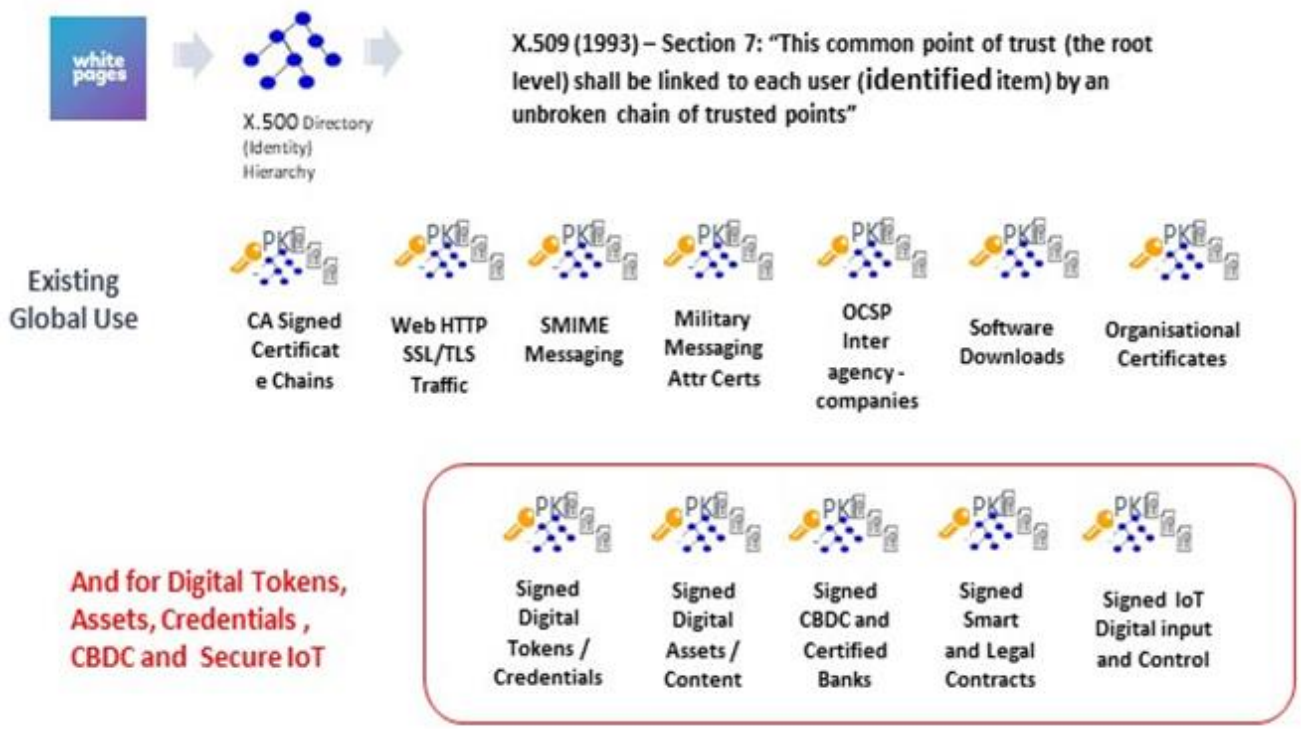
The key question with digital assets is: what are the content signing functions and what are the (identity) trust anchors they are legally tied to.

Question: Is the digital asset being digitally signed with technical level server keys or by the legal entity – the organization using a formal and managed Certificate Authority.



A good start to the ZTA initiative is – check the management interface of every server and application that uses PKI functions.
One may find these are engineer oriented configuration files or command line scripts ..
This UX/UI needs improving . Otherwise an easily managed system inc ZTA is probably impossible.

The current and future state of the worlds global PKI systems



The PKI in cuublemesh is a smart mesh cross node PKI which is integrated with its Operational Support System (OSS).
Both these functions work with the multi node - credential chain management functions and assist with the validation, management and transfer of digital assets between users, chains and nodes – they provide provenance and tracing.
5G Edge systems wont escape the use and management of PKI and trusted identity functions …..

Note: Many regulatory documents are requesting that digital identity and signatures are used on Tokens, Assets, CBDC, Contracts, Legal Documents, Smart Contracts and IoT device information and these may require several references for provenance and traceability. Cyber security issues and ZTA enforces such demands.

The Cuublemesh OSS – PKI (and ZTA) Management Functions (1)

Expanding the OSS views of the digital credential chain admin charts

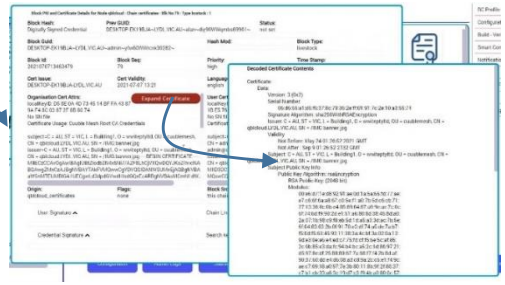
Displaying credential chain entry and its content, signatures and certificates.

Other features provided including certificate chain validation functions

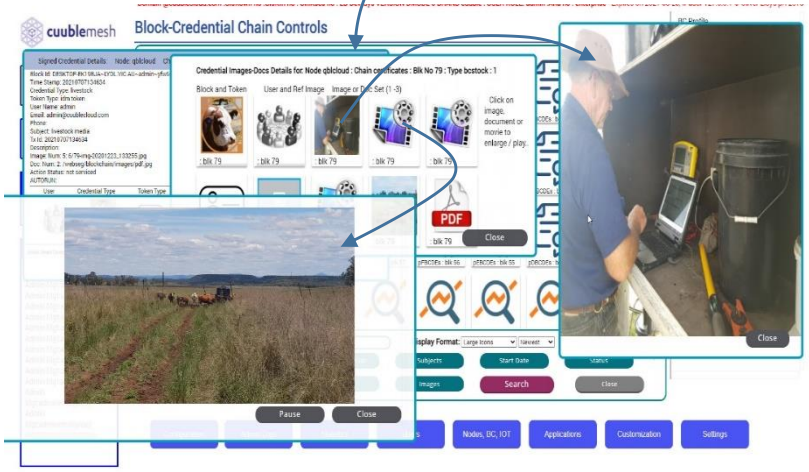
Admin: Viewing the PKI and Credential Chain(s) usage

Viewing the digital credential header and its 3 signatures

Expanding the credential header certificates



The credentials content – 1 image, 3 movies and a PDF document



An integrated web engine allows us to design systems functions on the basis they are made click through and visible.
We see this as an essential system engineering methodology to managing identity, governance, OSS and PKI based infrastructures – i.e. easily see all the functions that exist in an operational system to enable it an protect it – all part of ZTA..

Administrator screen shots shown - being web – customizable.

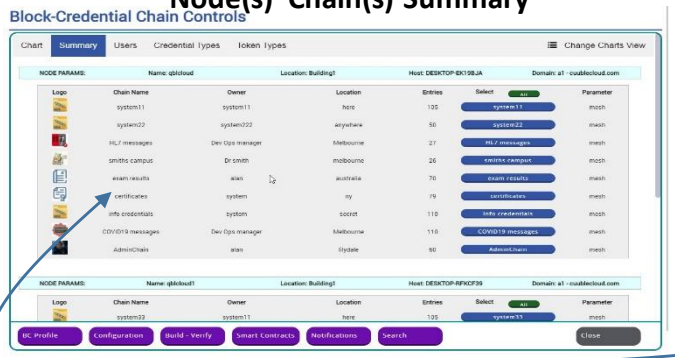
The Cuublemesh OSS – PKI (and ZTA) Management Functions (2)

Expanding the OSS views of the digital credential chain admin charts

Selecting Nodes, Chains, Users, Credential and Token Types.

Can also show illegal intrusion attempt details - logs

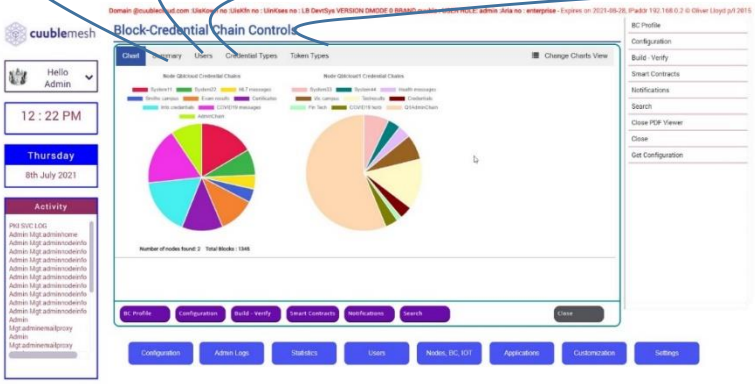
Node(s) Chain(s) Summary



Node(s) Chain(s) - Users

Node(s) Chain(s) – Credential Types

Node(s) Chain(s) Credential Token Types



Node(s) Chain(s) Entry Population Charts

Credentials carry a token type and schema – including 6 ITSA token definition attributes

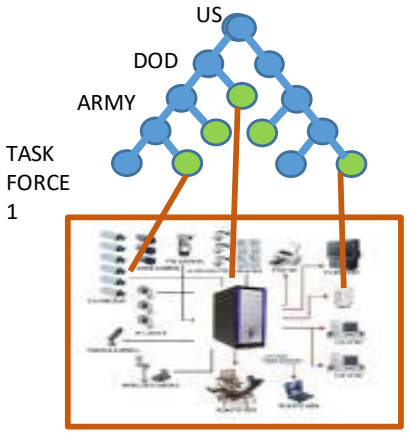
Real time visibility of the PKI system and its usage in action via the OSS is key – fundamental to ZTA too

cuublemesh

ITU X.700 and the ITU M. Series - TMN
Systems and Network Management and SNMP – the Internet Version

The X.700 (and X.500) standards are abstract specifications. They define an Object Oriented distributed information systems design, object schema and an systems engineering methodology. They do not define technical protocols, product or databases, thus the way in which these OO standards are used is up to the designer. SNMP was derived from CMIP X.711

Managed Object definitions
In this case we take our directory example and define that some of the identified objects in the namespace are representing network devices, 5G entities, configuration files, resource records and these 'objects' can also generate alarms and new services.
i.e **the green objects in the diagram represent identified devices**. Thus the system now is not just an identity structure for objects that exist for the users and application/system, but an identity structure for objects that ''are systems and networked managed, including infrastructures' and are applied in that way.



Systems Management Functions The X.700 standards specify functions, objects and attributes that enable coherent systems management. These functions are:

- fault management
- accounting management
- configuration management
- performance management
- security management

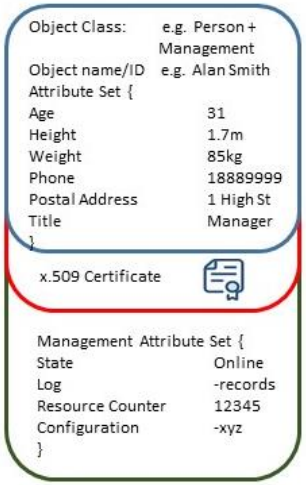
Note: Hopefully from the previously slides and this one, one can see why a web meshed engine platform with an OO ISO/ITU standards based information architecture, digital credentials, with an integrated PKI/OSS and IoT device interface, we basically have an identity/governed system with many functional dimensions which has considerable ZTA capabilities.

X.700 -The Managed Object and Operational Support Systems (OSS)

cuublemesh

All things in any system have an identity, are managed in some way.
Its best to use international standards so that such has structured design and engineering methodology

The Managed Object (basic)



Managed Objects defined in X.721 (for use as required within the OSS)

Alarm Record
Attribute Value Change Record
discriminator
Event Forwarding Discriminator
Event Log Record
log
Log Record
Object Creation Record
Object Deletion Record
Relationship Change Record
Security Alarm Report Record
State Change Record
system

CCITT Recommendation ISO/IEC International Standard

X.700 | 7498-4 (Note) Management Framework
X.701 | 10040 System Management Overview
X.710 | 9595 Common Management Information Service Definition
X.711 | 9596-1 Common Management Information Protocol Specification
X.712 | 9596-2 CMIP PICS
X.720 | 10165-1 Management Information Model
X.721 | 10165-2 Definition of Management Information
X.722 | 10165-4 Guidelines for the Definition of Managed Objects
X.730 | 10164-1 Object Management Function
X.731 | 10164-2 State Management Function
X.732 | 10164-3 Attributes for Representing Relationships
X.733 | 10164-4 Alarm Reporting Function
X.734 | 10164-5 Event Management Function
X.735 | 10164-6 Log Control Function
X.736 | 10164-7 Security Alarm Reporting Function
X.740 | 10164-8 Security Audit Trail Function

Object States, Controls, Logs and Events

Objects representing real things in a system, including organisations and users can change state, be off line/online, use resources, generate alarms, need configuration. Thus managed object attributes are needed.

X.700/X.721 cleverly allows for managed object definitions to have the same name – identity structure as the actual object its associated with. Therefore we can ghost/subclass the objects x.500 standard identity attributes with the x.700 system's management attributes and functions.

In this infrastructure systems engineering we have used OO defined systems standards where the objects represent real world entities and have identity, are assigned rights, can be validated as to being trusted and from an OSS perspective operationally managed.

cuublemesh

Realising Systems Management (X.700) in a managed meshed web system.

There are 100s of web screens/menu items with the cuublemesh OSS/PKI Admin functions. All easy to use, intuitive click through functions. That's why cuublemesh is meshed a web services engine..

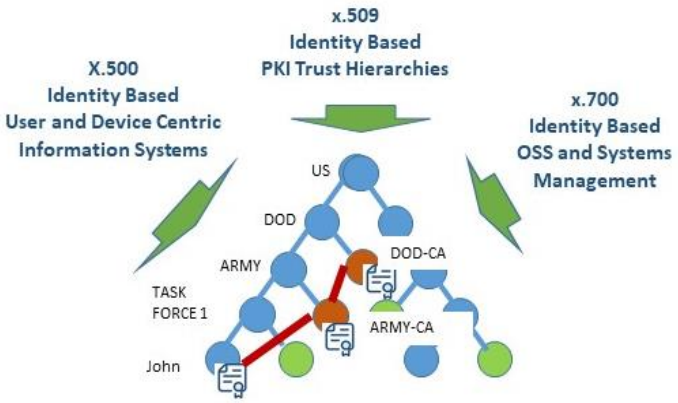
Fault management
Accounting management
Configuration management
Performance management
Security management

OSS Basic Functions

Don't build complex trusted systems unless they can be managed easily and quickly.

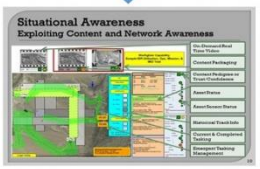
The collective – ITU x.500, x.509, x.700 and the genesis of cuublemesh

The ITU/ISO standards and engineering methods



Coherent, Interoperable Identity Based Systems Design – IoT enabled, Systems Management and Operational Contexts

The cuublemesh genesis: Mission based, trusted distributed information, identity engineered, robust, intelligence processing, managed, meshed, interconnected systems.



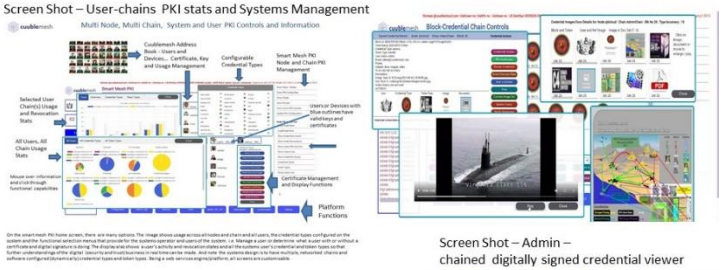
Theatre – Meshed C4ISR Nodes and Services Delivery

The Genesis of Cuublemesh
MAGTF 2011
USMC C2->C4ISR - Meshed Nodes, Information Engineering (Compute Area Networks)

Web Engines- Meshed Nodes, Information Engineering
Multi Chain Credentials
OSS-PKI, IDM and IAM
Aligning to USDOD ZTA

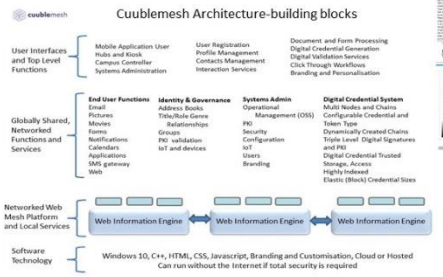
-- trusted ISRC4, a popup intranet if needed

Screen Shot – User-chains PKI stats and Systems Management



Screen Shot – Admin – chained digitally signed credential viewer

Cuublemesh Architecture-building blocks



Screen Shot – Admin – chained digitally signed credential viewer PDF and documents – and document signing , credentialising and forwarding- supply chains, command lines..

Identity, governance and systems management design, define scale, trust and operational utility.

The Web Page Document Object Model (DOM) and OO software languages

And :

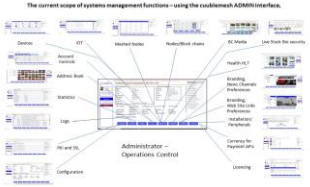
- **Cuublemesh identity centric and user information functions**
- **why cuublemesh is a meshed web engine**

The Digital Asset/ Content function

The Identity System – address book

The PKI Management Function

The Systems Management Functions



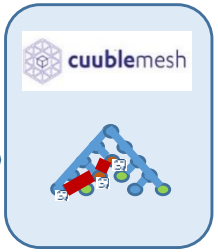
The web page DOM model uses HTML which includes Headers, Buttons, Divs, Lists, Images, Forms fields etc.
Within the HTML web page definitions each item can have a Class and an Identity
**e.g. This is a div **

Thus such lines in web pages (most of them) are defined and managed as objects. And to create, remove, display, change or act on these web display objects we use Javascript, JSON, Jquery and CSS and the browsers on screen/mouse event system.

Web Pages

Javascript, JSON, Jquery and CSS

Meshed Web Engine



The HTML-JS processes interacts with the cuublemesh meshed web engine via trusted identified session controlled mico-services via user or systems management sessions.

The cuublemesh 'identity directory' therefore is not just its address book but a composite of most things in the engine including its digital asset credential chains, documents/content , and system branding tools.

Object Oriented software languages C++, Java
- an information engine

Because the web engine is natively IoT and addressable, the identity system engineering is not just applied for authenticating users, it is applied to everything in the mesh so the mesh can work as mesh in a uniform, trusted, managed, scaleable and interoperable way.

User Interaction, Content Management and Mesh applications

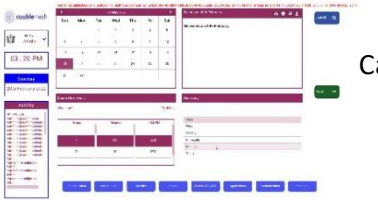
cuublemesh

The platform and its support functions provide a rapid POC development and a transformation and ZTA strategy environment.

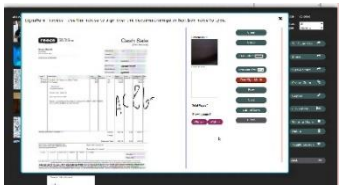
Address Book (essential)

Document Management

Mesh Application: Aged Care



Calendar(s)



Form Filling, Content Signing Provenance Credentials

Mesh Application: Campus Manager

Movies and Pictures

Mesh Application: Livestock Management

Mesh Application: Health Hl7 Patient Journey

Email (essential **)

Mesh Application: Investor Groups Documents and Contracts

Mesh Application: Social Hub

** email addresses are used in most online systems as the key identity anchor.. E.g.. forgot password functions.

Digital Transformation and ZTA with cuublemesh (1)

A quick start to a low risk digital transformation strategy and ZTA

Diagnosis Approach

- **Poor and Inconsistent Data and many data silos**
- **Insecure or poorly managed internet access and web servers and certificates**
- **Old document and form designs**
- **Old data management processes**
- **Poor Identity management and access systems**
- **Poor document signing processes**
- **Poor approaches to Internet security**
- **Poor approaches to digital asset management**
- **Poor approaches to online customers and their experiences**
- **Not sure what the costs of the above are to the organisation's OPEX**

We use the platform to:

- establish and test a de-silo agenda for data sets for optimum usage and value
- **establish greater levels of security through our OSS (and PKI) systems management platform**
- consolidate and web-enable document and form designs, usability and workflows
- **consolidate and web-enable the data owners and user management OSS (and PKI)**
- **revisit your identity system for interaction use, trusted relationships , PKI and Zero Trust Architecture standards adoption.**
- apply our platform's document(and image) electronic and digital signing functions
- apply the platform's unique multi node, multi chain digital credential and proof of provenance system
- recreate the user's experiences for services portfolios and self care, personalization and digital asset creation
- identify the costs saved with business intelligence systems using our trusted 'information pedigree' agenda

Digital Transformation and ZTA with cuublemesh (2)

cuublemesh

What we do

Proof of concept and proof of strategy

We capture the problem space for online systems operations, use and utility, TCO and ROI and trust-value systems and use our platform's existing functions to demonstrate how the legacy functions and processes can be evolved and demonstrate the value benefits in line with the transformation agenda. We also identify functionality and software which can be incorporated into legacy systems.

We do not affect operational systems for updates, modifications or replacements until well justified by our process, operational demonstrations and agreed with management

Where necessary we develop new code modules on cuublemesh in order to demonstrate how these new functions operate.

Diagnosis

Capture the scope of the work, its context, the perceived problem spaces and desired change and outcomes.

Identify what in the legacy systems and processes are the problem and then what technically can be operationally updated.

e.g. If document, content and data forms and their processes are the issue, capture the set for normalization and web services enablement using our document normalization functions/approaches.

e.g. If customer centricity, experience, product portfolio and the web services front end and identity management and trust systems are fragile, identify how OSS style functions can rectify such.

Finish and Thank you

In closing ..
I do hope the presentation material has been useful, it does represent some years of working with the standards bodies, the larger infrastructure style information systems and security and some great teams.

The journey…
I engaged with the ISO/ITU x.500, 509, x.700 standards as a result of ICLs work on OSI as started by Jack Houldsworth. His achievement, normalizing the networking and systems language for the world's ICT industry, its distributed systems engineering and standards developments - was foundational even for the internet. I worked with Jack on a few occasions, even at the ISO/ITU- IETF liaison level . See RFC 1888.
In memory of Jack.

I started cuuble then cuublemesh because of my aging Mum and her friends basically being intimidated and isolated by the IT transactional , business data systems and the micro button web interface agenda. Story at https://cuublecloud.com/papers/futureMakers-Social-Cells.pdf
In memory of Mum.

The new online world we are entering requires trusted managed and self managed global interoperable, multi nodal online infrastructures for many applications and the whole of society and ZTA is a part of that.

We are open to assisting with major projects, ZTA strategies, providing webinars of the material presented, investors or a trade sale of our platform technology.

cuublemesh

Additional Slides For Your Info

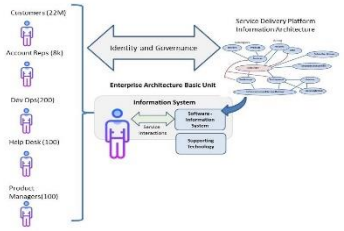
- ZTA – Systems Design Flows
- Cuublemesh features
- Signed Credentials
- Documents, Signing and Credentials
- Documents, Signing and Credentials Apps
- Credentials , Digital Assets, NFTs and Smart PKI/OSS – the Utility

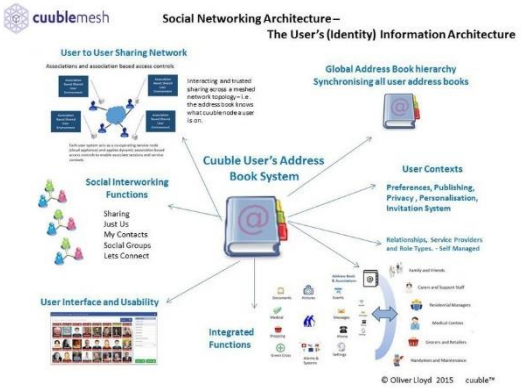
cuublemesh

Human centric, Top Down, Distributed Information Systems Design, Identity, Governance Trust.. Does one design a system with a database transaction knowing that such a transaction type has a limited life time. Or design re people interactions with a trusted services environment which can evolve because the interrelationships and trust aspects are dynamic.. And where the digital credential system is not a silo, but a standards based, system wide and personally controlled set of services and environments?

Problem Space – Determine how users and devices interrelate and trust each other, their roles, titles, services and the numbers of them. Service Delivery

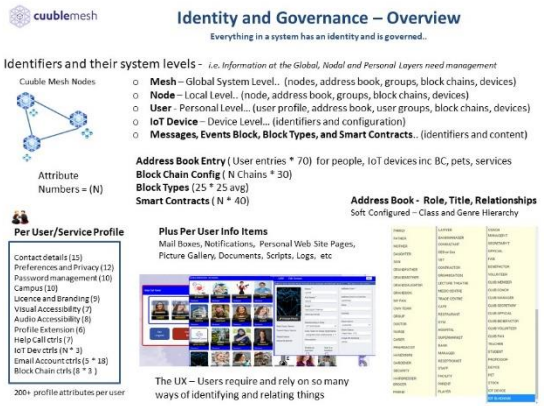
Problem Space – people use 30+ web sites- businesses – their data everywhere. Too hard for many.

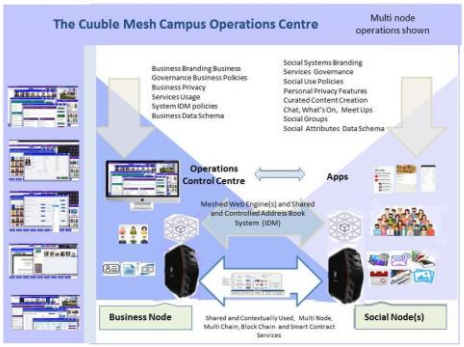




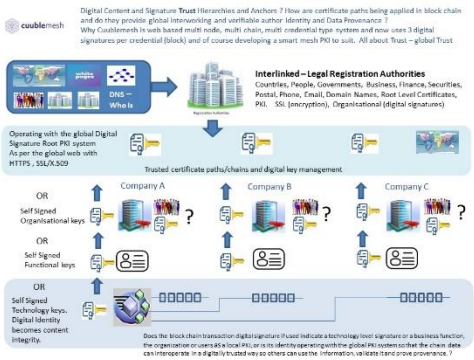
Information Engineering Step 1
The cuublemesh web engine (a UI/UX up front) and the address book system: the who, what, why, identity, governance, roles, titles, privacy and trust. The address book - 2 years to design.

Information Engineering Step 2
Soft configured role class hierarchy methods. 3 logical and interworking levels, GUI self managed, e.g. 68 Role / Title names configured -Users, Services, Groups, Devices and IoT and Chains.
i.e. Embrace multi node, multi chains as IoT identities.

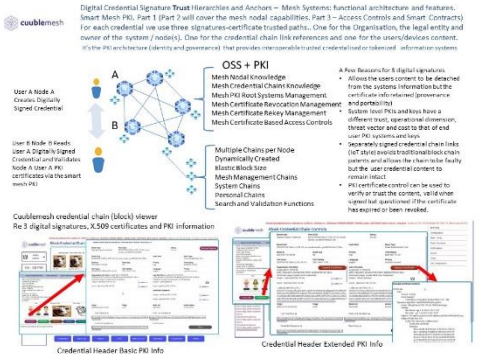




Information Engineering Step 3
Operations Centre, OSS, Decentralised meshed nodes allowing separate governance entities , users and services to interrelate and interwork.



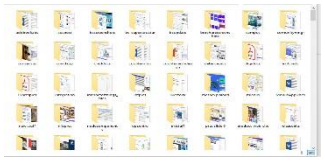
Information Engineering Step 4
Defining the trust hierarchies required for digitally signed content and X.509 certificate paths at scale, the use case dynamics of digital trust – the key systems , the credential chains, the users and devices.



Information Engineering Step 5
Address the large scale dynamics of PKI and key management, cross agency and mesh smart operations based on our 3 digital signature per credential chain(s) and OSS/PKI design.

Documents, Signing and Credentials

PC Platform Screens



1. Your PC files (pdfs and images) are uploaded to the platform and into your user document environment.

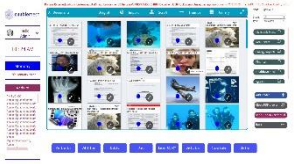
2. The document of interest is selected and placed in the signing /action gallery

3. The document of interest can have its signee list and caption added

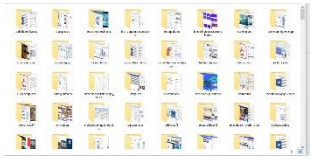
4. The document of interest is converted to single image pages for mark up using text boxes or pen /scratch signatures.

The credential chain and credential type is selected for the saved document and /or messaged to the recipient share list.

5. The credential chain entry is examined and the page images and new pdf document shown.



6. The new PDF document is written to the users document environment with a reference to the credential chain entry.

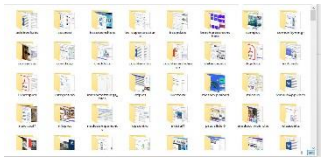


7. The new and signed/marked up PDF document can be downloaded to the Users PC environment.

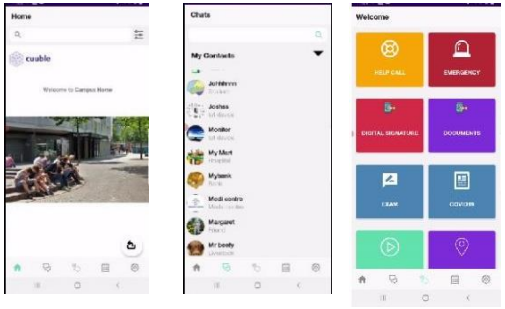
Documents, Signing and Credentials – the App

PC Platform and App Screens

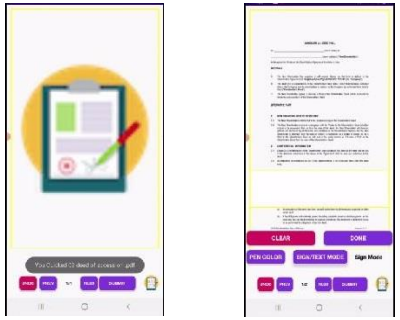
1. Your PC files (pdfs and images) are uploaded to the platform and into your user document environment.



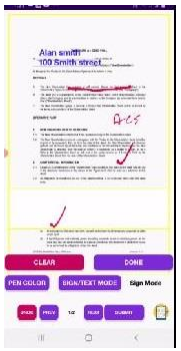
2. Log in and chat to other users re the documents /images. Select the document sign feature



3. The document of interest is selected and placed in the signing /action gallery for text and scratch signing on each page.



4. The document of interest is converted to single image pages for mark up using text boxes or pen /scratch signatures. Pen colors selectable.



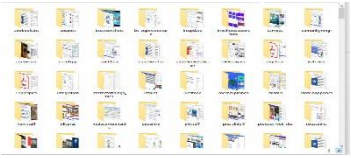
The credential chain and credential type is selected for the saved document and /or messaged to the recipient share list.

.

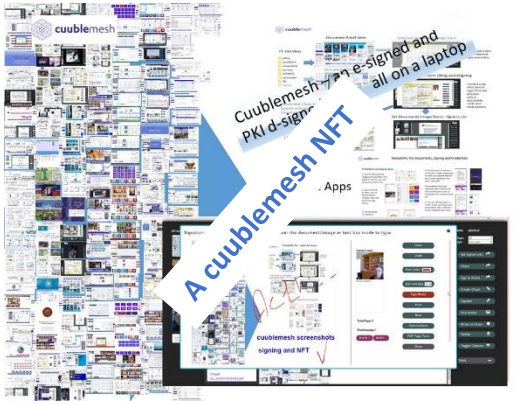
5. The new PDF document is written to the users document environment with a reference to the credential chain entry.

6. The credential chain entry is examined and the page images and new pdf document shown.

7. The new and signed/marked up PDF document can be downloaded to the Users PC environment.



Credentials , Digital Assets, NFTs and Smart PKI/OSS – the Utility



- With elastic block/credential sizes cuublemesh can hold collections of documents, forms, images, voice and video within the digitally signed credential – absolute legally verifiable proof of provenance credentials (above). Support food production, NFTs (upper right) with systems management (lower right).

- Cuublemesh uses (block) credential and token types where the token type can indicate the contracted financial details of the credential/digital asset.

Administrator screen shots shown Being web – customizable.

With a multi node, multi chain system, it means the integrated Credential chain(s), PKI/OSS functions are designed so that the systems administrator can see what is going on with the Users, Digital Assets , PKI functions across THE SYSTEM and manage the systems keys and trusted PKI certificates of course. Foundational for ZTA.