7 – The Building Codes Component

Question 7 *By what standards are we assured that an information facility is habitable, that is, secure and manageable?*

Answer 7 The Building Codes Component

Your information is never secure in a private, cryptographic tunnel if it is exposed at the ends of the tunnel. Indeed, a tunnel can be less secure than the outdoor space around it, because it gives its occupants a false sense of security. Building codes are sets of standards and procedures that ensure the integrity of the virtual buildings that enclose, for example, the ends of tunnels.

Highways and Buildings

Highways and buildings are nicely complementary. While we fondly recall trips to seashore and mountains, in fact people use highways mostly to go from one indoor space to another. Most buildings would be useless without a system of roadways bringing people to them.

I am a huge fan of the Internet. The old "information highway" metaphor still fits, and that highway just gets better and better. We all know the Internet has problems; bandwidth, latency, address space, lack of priority of packet forwarding, addressing, all present great challenges. As past challenges have been overcome, surely the present ones will as well[76]. In spite of its problems, the Internet is a sound highway system with plenty of room for growth.

But there is a much bigger set of problems, not with the Internet highway system itself but with the assumptions that a public highway system can be used for things for which it was never intended.

The Internet's basic nature is to serve as arguably the greatest public facility ever conceived, and it fulfills that role every day. But it fails when it is expected to be more than that. The problem lies in assuming that once the highway is built and smoothly carrying large volumes of traffic, we're done. In fact, we haven't really started; we haven't begun to build the buildings.

While we need online facilities with all the benefits of spaces defined and designed for specific uses and specific groups, what we have is a vast collection of roadside stands

[76] For perspective on this, read Bob Metcalfe's 1996 prediction that in 1997 the explosion of demand for video and audio media would bring the Internet to a grinding halt. No one is more qualified than Bob Metcalfe, inventor and perfecter of Ethernet, founder of 3Com, distinguished technology journalist, and rich-from-placing-the-right-bets Internet entrepreneur, to talk about the future of the Internet. But when it came to predicting its capacity, he was dead wrong.The average technologically unsophisticated individual who bet a couple thousand dollars on a home computer solely for experiencing the new multimedia Internet was, it turns out, dead right.

called “commerce-enabled websites” and detached reception areas called “portals.” We have strained mightily to make a highway do the job of a building.

It’s time we acknowledged the value of boundaries.

We Don’t Have to Love Walls to Need Them

Robert Frost’s famous poem “Mending Wall” makes an important and timeless point about the desirability of boundaries. “Something there is that doesn’t love a wall.” Frost laments society’s tendency to want walls, and pokes fun at his neighbor’s insistence that humankind is better off for the walls and fences it erects. Frost would be at home with the open rangeland culture of the Internet.

As much as we do need walls, we also need the poet’s idealism. We must take steps to ensure that people like Robert Frost are accorded protected spaces where they are free to be poets. We’re all better off if we recognize the utility of walls and admit that they are a practical necessity for most human discourse. We don’t have to love them.

It’s Not about Civil Liberties

The content of the Internet — that is, the nature of the activity for which people use the information highway — is ungovernable. That has a certain appeal, doesn’t it? It goes along with the open rangeland mentality that accounts for the aversion to boundaries. No government, no boundaries, “information was meant to be free” and all that. It’s simplistic, but it’s based upon a good principle: Public spaces, even regulated public spaces such as roadways, should not impose arbitrary limits on the freedom of their users.

But that does not mean that the facilities to which the highway takes you are ungovernable. The use of buildings is governed by the adoption and enforcement of rules that apply when you go from outdoor space to indoor space.

Surprisingly, the First Amendment is often invoked on this issue, as though creating a building and restricting access to it denies constitutional rights to those who are not invited in. But policing behavior in a meeting room is appropriate in ways that would never be appropriate in a public space. The person in charge of the meeting can ask you to leave; it’s not a question of rights or freedoms or civil liberties, it’s a question of what’s appropriate in that room according to the judgment of the individual who is responsible for the meeting.

Picture a hotel and conference center adjoining a public park. An individual may say and do what he wishes in the park, where the police concern themselves only with illegal behavior. In the hotel lobby, he may say and do what he wishes so long as he is not disruptive. The hotel is in charge of that space, which is known legally as a public accommodation, somewhere between public and private. In the general area of the conference our guest is expected to wear a badge showing his name and affiliation to other conference attendees. In a room where a session is underway, the moderator maintains an even greater level of control, which has very little to do with First Amendment rights and a lot to do with the purposes for which the room is dedicated at that moment.

The Microsoft Office Complex

How do Microsoft and Apple relate to the community of partners, software developers, businesses, and customers they work with? How do they relate to companies that they consider rivals, or rivals of their allies, or simply companies that present a view of the world that is at odds with their own? The clue is in their "architecture."

.NET HailStorm and Palladium were strategies masquerading as architectures. They were covers for agendas by which Microsoft doles out favors to some organizations in exchange for an icon or a software routine that does not discourage the user from using the sycophant's product.

Real Architecture

In order to build and use viable online buildings — to obtain Quiet Enjoyment — we need tools and building materials that are up to a standard and that work together. When we are invited to participate in an online meeting in a facility we have not visited before, we need to have confidence that what we say in that meeting will not be exposed to the whole world and that the people we say it to are who they claim to be.

As it is, there are not only no building codes, there is not even a common language for discussing blueprints. The way it works now, a set of drawings has to be specific to one specific contractor and often one specific supplier of each type of building material. They are not substitutable.

Can you imagine if the architecture and construction and building materials and real estate industries worked that way? A set of drawings would only work with one vendor of building materials and could only be interpreted by one contractor.

Conversely, if we have a standard vocabulary and a standardized set of methods and procedures for online architecture, construction, building materials, and property management, we can start building buildings and enjoying their use.

Some of the folks at the World Wide Web Consortium, Oasis, NIST, ISO, IEEE, or other standards bodies would take issue with that. They've been developing standards for years that enable computers to interoperate over networks.

Once again using the world of physical real estate as our guide, suppose you were to say to a building inspector, "All of the materials that went into the construction of this office complex are certified to be compliant with all relevant standards and codes, so please give me my occupancy permit." She would likely answer, "I see a bunch of high quality code-compliant beams and framing and concrete and wiring and plumbing thrown together in something that vaguely resembles a structure that is obviously not code compliant. You'll have to start over, putting the materials together in a manner that meets code."

The business of construction materials and the business of construction require different sets of skills and knowledge. A contractor need not know the first thing about the manufacture of particle board, but must be thoroughly familiar with the fact that you can't put point stress on it as you can with plywood.

This Is Not New

Some established knowledge about the construction and management of online buildings has existed ever since the first special interest meeting-places — social networks with architectural features — were built in Delphi and The Source and CompuServe and EMISARI and EIES in the '70s and '80s. But until the Web came along, such knowledge was squirreled away among the managers of special interest areas in those online services. (BBS sysops managed some smaller buildings as well.) There was no established profession, which is what engenders meaningful standards and common procedures.

That started to change as the Web matured. The World Wide Web is a remarkably complete collection of reception areas of most of the organizations in the world. The professional Web developer has a portable set of reception room construction skills, consisting of a fairly light understanding of the way construction materials are built and a much deeper understanding of the way a semi-public space must be designed in order to be of greatest help to visitors and occupants. The professional webmaster has a parallel set of property management skills, applicable mostly to reception areas.

As we have noted, identity is not particularly important in a reception area; identity is what is established in a reception area if someone wants to go past the reception desk into the workspaces beyond. If you simply want to pop in and grab a brochure, you can typically do that without leaving a business card.

When in the online world we go past the reception desk, we leave the area covered by the professions of Web developer and webmaster. The VPN/intranet/B2B exchange/extranet space remains in the dominion of the IT professional, i.e., the construction materials professional. Since these people consider security to be a military matter rather than an architectural matter, users of that space must be prepared to try to get their work done on a battlefield, devoid of the benefit of professional architects; a space where it's assumed that everyone is either friend or foe rather than a well-identified person who is accountable for his or her actions while there.

We need three things. First, we need an understanding that a secure space is a facility, an online counterpart to a physical building. Second, we need a set of building codes by which such a space can be judged and certified as secure — that is, manageable.

Third, we need nomenclature that can be used to identify and specify (describe with specifics) a facility that is code-compliant.

Introducing InDoors™

Having standardized names for elements of a facility is more important than it might seem. In Chapter 16 we noted the term "relational database" and the database management systems that claim to be relational. E. F. Codd, the inventor of the relational database model, listed 12 standards that a database management system must meet in order to be considered relational. He also was involved in the creation of Ingres, one of the early relational database management systems.

The fact that a database management system must pass Codd's 12 tests in order to be called "relational" means that the term can be relied upon. It's not up to some writer of brochure copy, it's up to the person who coined the term.

Without a definitive term, a noncompliant vendor skilled in FUD techniques can claim, for example, that its database management system works in relational ways and therefore is a relational database. That would defeat the whole purpose of creating an element of language through which people who build and manage buildings can reliably share information, tools, and building materials.

To prevent the kind of FUD-induced linguistic corruption found in most information technology, we introduce the terms "InDoor™ facility" and "InDoors™" to refer only to a code-compliant building or set of buildings.

While an InDoor™ facility exists only online, that fact does not define an InDoor™ facility. For example, something that starts with an icon of a city which, when clicked, brings you into a virtual-reality "experience" where you buzz through classrooms and offices and homes is not an InDoor™ facility unless it meets InDoor™ requirements.

An InDoor™ facility is defined by function, not appearance. An InDoor™ facility lets a project manager quickly and easily set up a controlled meeting room, delegate management of the room to one of its members, set up the access control list, and, most importantly, provide the tools to effectively manage the space.

A Mental Picture Explains All

InDoor™ spaces are not defined by new technology. Indeed, the technology is mostly the same old stuff of which SSL tunnels are made.

Really, there is not much more to the difference between a tunnel and an office building than is revealed in a mental picture of the two. So picture a tunnel and then picture an office building. The tunnel has both outdoor and indoor characteristics. Although the center of the tunnel may be considered to be indoors, you wouldn't do the usual indoor things there. You wouldn't set up cubicles or classrooms inside a highway tunnel, or transact business there.

Now picture an enclosed pedestrian bridge between that office building and another building. The pedestrian bridge is part of a barbell-shaped object, the two buildings being the "weights" and the pedestrian bridge being the "handle" of the barbell. Topologically it is an enclosed sphere.

The tunnel, on the other hand, is a tube, which is topologically a donut shape; the hole represents the whole outdoor space.

You can see an animated illustration of this, with a highway tunnel morphing into a pedestrian bridge between office buildings, at about a minute into the video at http://www.youtube.com/watch?v=tAnvZKAyDZ4&feature=relmfu. (While you're there, you can watch the whole series of QEI videos.)

Really, there's not much to the essential idea of InDoors. If you know the difference between a tunnel and an office building, and you know how to use them, then nothing essential remains to be defined.

So let's move on and look at the different uses of InDoor™ facilities and the forms they take.

Basic InDoor™ Facilities Specifications

A facility may be considered to be InDoors™ if it meets the following specifications:

1. An InDoor facility is identified by a globally unique Facility ID, registered at the City of Osmio Buildings Department.
2. Each InDoor Facility is at any particular time the responsibility of the Property Manager whose Osmio VRD credential is associated with the Facility ID in a file within the facility itself. It is available to anyone on that facility's Access Control List. The Property Manager may be an owner, an individual tenant, or an individual designated by an owner or tenant.
3. An InDoor facility carries an occupancy permit, which takes the form of an X.509 certificate containing the Facility ID and signed by the Osmio Buildings Department.

In order for a Certificate Signing Request (CSR) for an Occupancy Permit to be considered by the Buildings Officer, the CSR must be signed by three professionally licensed individuals:

- a professionally licensed architect
- a professionally licensed contractor
- a professionally licensed building inspector.

Each InDoor facility is accompanied by an Access Control List (ACL) containing the public keys of all who are permitted unescorted entry into the facility's InDoor spaces.

In addition to InDoor spaces, a facility may include public spaces such as yards, lobbies, showrooms, retail areas, and anonymous meeting places such as bars. No identity credential is required for entry into public spaces, unless their owner or manager specifies otherwise.

Types of InDoor™ Facility

One reason for having measurably reliable identities is to enable people to work and play in confidence in spaces that meet their needs.

There are two types of facility: **Personal Facilities and Group Facilities.**

Personal facilities include:

- Residences
- Personal offices
- Dens
- Living rooms

Group facilities include:

- Public office buildings
- Commercial office buildings
- Office suites
- Meeting rooms
- Filing rooms
- Cubicles and private offices
- Desks
- Cafes
- Bars
- Libraries
- Schools
- Clubhouses
- Houses of worship
- Showrooms
- Retail stores
- Retail malls
- Arenas

Some of these typically belong inside others. For example, a cubicle belongs inside an office suite, which belongs inside a public or commercial office building, which belongs inside a community. A Personal Office belongs inside a residence.

Personal Facilities may be entered via a browser, while Group Facilities require the Door™ client program. Additional requirements that apply to Group Facilities, also called P2P Facilities, will be described below.

1. Personal Facilities (Residences or MyOwnProperty)

Residences are characterized by the fact that all content is under the control of the owner of the building and his or her close family. P2P architecture is not required.

A Residence, also known as MyOwnProperty, may be built in a residentially-zoned district in a Village® authenticity-enabled social network. It conforms as much as possible to the APIs of other social networks so that a Residence may be made as accessible to, for example, a Facebook user.

The outdoor presentation of a residence, or MyOwnHome, will be invoked directly via

1. a browser
2. the Door™ P2P client software
3. a Facebook API
4. a Village®API

The owner of a residence is in charge of its access controls and privileges and, to the extent that custom design is provided in a given model, its exterior and interior design. Those privileges and responsibilities may be delegated by the owner to one or more tenants.

The residence may be identified and found (addressed) by the owner's or other residents' Facebook ID, OpenID, iName, or any of a number of other SSO identity credentials.

The variety of residences will be like the variety of residences in physical space, including

1. public housing studio apartment
2. public housing, multiple occupant apartment
3. apartments for one or two adults and multiple dependents
4. detached single family two-bedroom home (up to two adults and two dependents)
5. detached single-family three-bedroom home
6. custom home

A MyOwnProperty facility, or Residence, will be hosted on at least two nodes: a workstation and a directory on a remote server that are under the direct control of the owner of the MyOwnProperty. One of the two is designated the Principal Node and is the authoritative source of access and privilege information.

A Residence will include MyOwnYard, visible to anyone. Owner of the residences can decide whether to make their names visible.

The owner of a residence may apply a CRL to the yard, or require an Osmio VRD identity certificate with a minimum Identity Quality score for entry, or waive entry requirements. "Entry to the yard" means the ability to cross the graphical representation of the yard and click on the door of the residence.

If the Residence is part of a condominium, co-op, or apartment building, the yard is shared and has no access restrictions.

MyOwnHome consists of a series of graphical elements that suggest a physical residence. The owner of a MyOwnHome may add images from a physical home, as well as other devices such as a bulletin board where visitors can leave messages and engage in discussions with the owner and each other.

A MyOwnHome carries an ACL that includes the public keys of those who are permitted to enter at any time and those who are permitted to enter during designated visiting hours.

The owner of a MyOwnHome may invite in others who present valid Osmio VRD identity certificates. The Identity Quality score of the visitor will be visible to the owner in that circumstance, and clicking on the score will bring up the eight Identity Quality component scores. The owner may request the visitor's name and personal information (such as gender or age), which the visitor may then license to the owner.

Each adult occupant of the residence will also get one MyOwnOffice; the only public key on the default ACL of the MyOwnOffice is that of the occupant named as the owner of the MyOwnOffice, not necessarily the owner of the Residence. The owner of the MyOwnOffice may add others to the MyOwnOffice ACL (e.g., spouse or assistant).

Each office includes MyOwnInformation, a file cabinet containing personal information about a particular individual. It is designed to implement the methods, standards, and features of the Personal Information Ownership Component of the Authenticity Infrastructure ("People") part of the Quiet Enjoyment Infrastructure.

The assumption is that there will be one MyOwnInformation file cabinet for each dependent in the household.

All information in a MyOwnInformation file cabinet will be encrypted by an AES symmetric key that may be released for use only by the owner's (subject's) Foundational PEN®, utility PEN® or device PEN®. The owner may request that a copy of the encryption key be shared with a trusted acquaintance or Attestation Officer in case of loss.

The MyOwnInformation file cabinet will include the following file drawers, which contain information in modified SCIM format:

Biographical reference work: Personal information subject to the copyright law of all jurisdictions that subscribe to the International Copyright Convention

My Own Body: The subject's health records

My Own Relying Parties: Information about those who have signed the subject's PersonalNDA and been granted a license to particular items of information, including date of issuance of the license, items of information licensed, purpose for which the information can be used, an expiration date.

MyOwnCredentials: Facilities for generating new Certificate Signing Requests from a Foundational Puzzle Kit (foundational certificate and its PEN®); facilities for managing Identity Quality information, for arranging IdentityQuality upgrades and for disputing Identity Quality decisions of Attestation Officers; contact information for individuals who have copies of keys and passwords; keys and passwords of others given to the owner/subject for safekeeping; MyOwnCircles, contact information and files about colleagues and acquaintances that are not to be shared; MyOwnWork (files being worked upon) and other files defined by the subject: and MyOwnAssistant.

All information inside a MyOwnOffice may be licensed by the owner to other parties.

The relying party must sign the owner's PersonalNDA with the PEN® associated with the relying party's Osmio VRD credential. (Note that only individuals are issued Osmio VRD credential; organizations must appoint signing officers who accept personal responsibility and liability for the organization's performance on the terms of the PersonalNDA and associated licenses.)

The licensing and signing of the digital documents will be managed by a robotic MyOwnAssistant, who will respond to requests via a "drive-up teller window" facing outdoors. When a digitally signed request is presented, the Assistant will check for a digitally signed PersonalNDA and license to the information requested.

If no NDA is on file, your assistant will present your PersonalNDA form, which includes spaces for identifying which items of information are requested.

If an NDA exists but you have not issued a license that covers the specific information requested, your assistant will ask the supplicant (that is, the relying party) to fill in and sign a new PersonalNDA with the additional items identified. My Own Assistant™ consults My Own Disclosure Instructions™ which in turn is based upon a table that is produced by the signing of PersonalNDAs. My Own Assistant™ consults My Own Disclosure Instructions™ any time anyone asks for personal information. "He or she" then follows those instructions explicitly.

The MyOwnAssistant and the supplicant will normally be pieces of software that talk to each other via an API. In such case the information exchanged is in an XML-based personal information markup language, PIML, which is based upon SCIM, as illustrated in the chapter describing the Personal Information Ownership Component.

2. P2P Facilities (Facilities for Groups)

As the name implies, a P2P Facility, or a facility within a P2P building, must accommodate file cabinets that are under the control of different people.

1. Group facilities consist of office buildings, meeting halls, clubhouses, libraries, bars, and others. A group facility is built upon peer-to-peer technology; it may be hosted by both a local machine and any number of remote machines, but it appears to the visitor as one integral space. One of the machines, designated the Principal Node, is the authoritative source of access and privilege information.
2. An InDoor facility must be constructed of code-qualified construction materials, as designated by the City of Osmio Buildings Department. Such code-qualified construction materials exhibit the following characteristics:
    - All communication among machines is encrypted using symmetric keys established through a key exchange initiated by use of x.509 certificates identifying each machine (see Skype protocols) and facility.
    - Within a machine, all InDoor content is encrypted with a key that is protected as specified in the PEN System.
    - The keystrokes in any machine that houses a node in an InDoor facility are

encrypted by means of GuardedID or equivalent.

- Access to and privileges within the facility have nothing to do with the physical machines or file systems where content happens to reside; rather, access, privileges and responsibilities are defined by Access Control Lists and Privilege and Responsibility controls.
- Parts of the facility are connected to each other via a specific P2P-based protocol, to be chosen from a list of ADC, Skype, or Inferno-based protocols and software, including Retroshare, wxWASTE, OceanStore, Inferno, and others. N2N may be used to include machines in NAT subnetworks.
- An occupant or visitor must use a code-qualified client program, called a Door, for entry into spaces other than public accommodations in an InDoor facility or Residence, which may be accessible via a browser for the forseeable future. The Door may reside on the same machine that serves as a node component of the facility.
- The facility may house files from any number of machines, provided they all adhere to these specifications
- An occupant must present a valid Osmio VRD credential of requisite Identity Quality for entry to any part of the facility that is not designated as a “public accommodation.” Public accommodations include floor display spaces in a retail facility, reception lobbies in office buildings, and yards in residential properties (MyOwnProperty).
  - » Requisite Identity Quality for entry is specified by the Property Manager. It may be designated as a minimal total Identity Quality (IDQA) score (0 – 72) or a minimal score on any or all of the eight components of the Identity Quality score.
- Facilities may be nested inside each other to an indefinite number of levels, but every nested facility has a requisite Identity Quality score equal to or higher than the level within which it is nested.
- Navigation between InDoor spaces is as follows:
  - » Between connected corridors or hallways.
  - » Between unconnected InDoor spaces by means of “teleport” (clicking on a list of InDoor spaces that the occupant knows about) or via the outdoor roadway, i.e. a browser, to the other facility's reception area. Once the reception area of an InDoor facility is reached, entry is only by means of a Door client, not by browser.

The Door™ Client

The Door™ client program is built upon the code base of one or more open source peer-to-peer client programs. It is launchable only with a securely derived and passed ticket from the pre-launch program.

The pre-launch program causes a hash procedure (SHA-3 or Whirlpool or other suitable hash function) to take place on the Door client's executable code, and verifies its code signature before launching.

In the Door, as in any code used in the implementation of an InDoor facility, there is no such thing as software code signed by Microsoft or Apple. Rather, things are signed by an individual code signing officer, a holder of a professional code auditor's license, issued by public authority, who is compensated for the personal liability assumed. If the personally signed software code allows intrusions into your information home, the code auditor’s professional license and livelihood are put in jeopardy.

Signing officers will expect their employers to indemnify or insure them. But their personal signature will be as visible as the signature of the architect and contractor and building inspector on the occupancy permit of any building.

When the Door client launches, a window slides open from right to left, covering 90% of the area previously occupied by the browser window. The Door client window carries a thick border of a distinct color and pattern, always the same (acts like a trademark) with the words “You are InDoors” in the top border.

The Door client will observe occupancy permit rules and enforce all access controls, including ACL checking and Identity Quality checking.

Bars vs. Office Facilities for Groups

In the physical world, people don't often confuse an office with a bar. But online, people don't know they can have an office facility, and so they get a bar instead.

People who put up “collaboration facilities” quickly discover that office buildings just don’t have the same appeal as bars. Few people show up, and those that do treat the space like a bar, hanging out at the iconic water cooler.

The office is where we get things done. There should be specific expectations about team members' time in the office.

When people get together to collaborate, they need an office suite, with cubicles and meeting rooms and file spaces. The person in charge must be able to create and manage the facility with as little effort as possible. There is no role for a sysadmin in this process, except when the system crashes, which must be a rare occurrence. If the facility requires a sysadmin to be useful, it is not useful.

A few keystrokes by an untutored project manager or team leader must be all that is required to create a new facility, with its own access controls, privilege assignments, and responsibility assignments.

MyOwnBar, i.e. Blogs

Bars, like blogs, are often closely identified with their individual owners. There is an accountability threshold in both a blog and a bar; the owner would like to know who you are just in case you are involved in some trouble that calls for accountability.

Some measure of accountability usually is called for.

Basic Construction Materials

A reliable InDoor™ online office facility is built from the collection of construction materials and methods and standards called the InDoors Infrastructure, one of the three main parts of QEI. This means the foundation concrete, the sheetrock and plumbing and access control devices are made of PKI (puzzle kit infrastructure), reliable identities, professional licenses, building codes, and occupancy permits.

InDoors Vocabulary

Just as the sign on a conference room says “conference room” instead of “painted sheetrock,” InDoor facilities should be identified by their function rather than by the construction materials used to build them. It's not a “wiki,” it is a place.

Standard Office Suite™

These days hotel developers sometimes buy whole bathrooms as single units rather than a collection of fixtures and cabinets. It's a very efficient way to get a useful facility built quickly.

That's the idea behind the Standard Office Suite™. Whole rooms are installed rather than individual pieces. The Standard Office Suite™ consists of a minimum set of facilities that are necessary for the effective performance of a workgroup.

We will get into construction materials, but for now suffice it to say that the Standard Office Suite™ is designed to be configured, installed, and managed by anyone with permission to do so from a building owner or tenant. This is the plug-and-play of prefab office facilities. There should be as little involvement from coders and sysadmins as possible.

To illustrate, see http://www.delphiforums.com/ and click on Create a Forum. I have no idea how many tens of thousands of forums are hosted by Delphi these days, but if it took one minute of a sysadmin’s time to set up each one, it would be out of business.

Let’s assume the manager of a workgroup needs a Standard Office Suite™ placed inside an existing Standard Building. What does Standard Office Suite consist of? We'll really get into futures here; this is where we're going, not something available tomorrow morning.

Architectural Features of the Standard Office Suite™

The Standard Office Suite™ offers the following features:

1. File cabinet
2. Meeting rooms (at least one)
3. A shared calendar

4. A project management whiteboard
5. Desk for Manager of Customer Relations including:
   - Chart of Accounts
   - General Ledger and other ledgers
   - General Journal and other journals
   - Payables files
   - Receivables files
   - Reporting facilities
6. Boss's Desk
7. Researcher's Desk:
8. HR Director's Desk, with the following for each occupant:
   - Contact information
   - "See me about" information
   - Availability schedule
   - Anything else that's pertinent to the group
9. A MyOwnOffice™ cubicle or private office for each occupant. This is the same MOO that appears in the subject's Residence (aka MyOwnHome), with the same MyOwnInformation and the same MyOwnAssistant.

Each room is effectively a peer-to-peer facility whose security is governed by the Puzzle Kit Infrastructure that is built into the client device. Session keys are established after asymmetric (public key) validation is performed. The tunnel itself may be either SSL (TLS) or IPsec.

Each office suite sits inside an Indoor Space. The features of an IndoorSpace include:

1. Indefinite number of levels (rooms).
2. Selective rule-based inheritance of authentication elements from room to room (i.e., the management of a facility may allow the import of privileges from room to room, or may require each room to maintain separate access control lists and privilege lists).
3. Specific minimum feature sets for the standard facility and rooms within it.
4. Sensible, real-estate-based build-out tools and terms.
5. Effective and easy-to-use property management tools.
6. Works like a physical building.
7. All tools and terms are from real estate, not technology. Does not necessarily look like a physical building (not a navigation aid).

An InDoor space, then, is a building or an independently managed space within a building, or a real estate complex consisting of multiple buildings. An InDoor space may be small or large, simple or complex. A small group may only need a meeting room inside a building that is owned by someone else. Others may need many rooms, or a whole floor, or their own building or a building complex. A company may want its own building plus an office inside a Village® community owned by an audience aggregator such as a special-interest magazine that serves its industry.

If you were looking for a physical office in the real world, you would seek out a good commercial real estate salesperson, or a good architect and general contractor. But nobody is in the online real-estate business. There are plenty of people who know how to configure and install the software. But when you talk office layout, they talk IPsec.

We have no common language for online real estate, no set of rules by which the various elements interoperate.

So I will refer you again to the website where by definition the language of real estate drives all discussion. Come to abyxproperties.com to learn more about your specific next steps. Or, if you think you might be interested in starting an architecture, construction, real estate, or office management business based upon these concepts, feel free to contact me, wes@ReliableID.com.

The Model Office

Once you have your Osmio VRD Wallet with its embedded utility certificate based upon your Osmio VRD Foundational (Birth) Certificate, creating a facility is like creating a word processing file. It's as simple as File → New Facility.

Then you'll need to define who is allowed into your facility, either by listing them individually or by naming an authenticated group. Within that group certain individuals will need privileges, for example the ability to edit or replace files, to edit the access control list, or to manage the appearance of the place. Once you do that you have a basic meeting place.

If you want it to exist within another meeting place, and inherit its access control list as a starting point for making a subset, the manager will have to create it for you and then name you manager of the smaller space.

You can get a feel for the new real estate using any computer and practically any browser at abyxproperties.com. You'll find a complete conference center and expo hall, where you can check out what it's like to use online collaboration. You can engage in intelligent discussion with people you know, or know of, and be reasonably certain they are who they say they are.

You'll be "reasonably certain" because they will be using soft certificates, which means that really it's the computers rather than the attendees themselves that will be authenticated — unless and until you and your colleagues have an Osmio VRD Wallet.

This is adequate for some kinds of communication, but it certainly doesn't meet code. For important business meetings you'll need something much better.

If you are a developer (software, Web, database, etc.) you'll learn more about the professional side of the process in Chapter 25, "The Professional Licensing Component."

What's Involved in the Design of Buildings

Some buildings are built without any building codes, such as the favelas in Rio de Janeiro. Or the private networks of some Fortune 100 companies. They really have no idea exactly who those thousands of users are who purport to be employees of suppliers, distributors, partners, law firms, ad agencies, and the company itself.

Our building code starts with the foundation: all occupants must have an Osmio VRD Birth Certificate, which can be used to sign any other certificate or file, and therefore to access a building. There are boundary conditions where, for example, a reception area, i.e. a website, is accessible to both outdoor and indoor spaces. But to actually enter a facility, or to be put on a list of people authorized to make use of a meeting facility, the individual must have an Osmio VRD Birth Certificate.

The space itself must have certificates signed by the appropriate individual's Osmio VRD Birth Certificate. These certificates will provide the end user with assurance that the facility is indeed as secure as it claims to be. These certificates are checked by the programs that implement a facility whose configuration is defined by facility description records, which are in REML files.

Building Permit
Use: Authorizes the facility to exist on a particular machine and ensures that it is indeed located on this machine.
Signed by: The owner of the computer on which the facility is located.
Comments: Must be reissued if the facility is moved to another hardware server.

Title
Use: Provides proof of ownership of a facility. Links person to the facility.
Signed by: Owner, Registry of Deeds
Comments: Cannot be transferred; must be revoked and reissued.

Occupancy Permit
Use: The most important certificate, it certifies that everything about the facility is up to code and gives the facility the right to operate. This is the certificate checked by the client/end-user.
Signed by: Building inspector
Comments: Expires after a set amount of time. Also can be revoked if the facility does not pass an inspection and is not immediately brought up to code.

Lease
Use: Issued by owner, giving tenant the right to make use of the facility to a specified extent and for a specified amount of time.
Signed by: Owner, tenant
Comments: Expires after designated time. Can be reissued.

Municipal Charter
Use: Issued by the Osmio Provincial Authority to an entity that addresses a defined audience
Signed by: Head the Osmio Provincial Authority
Comments: Does not expire. Revocable only under certain circumstances.

The property certificates are issued in the form of Real Estate Markup Language files that are digitally signed with the PEN of a licensed professional architect, contractor, and building inspector.

REML: The Jargon of Buildings

Real Estate Markup Language is based upon XML. The REML represented here is barely a sketch, a list of REML entities that must go into the design, construction, and management of a facility.

Basic Real Estate Markup Language (REML) Schemas:
Facility Description Language
Role Description Language
Privilege Description Language
Responsibility Description Language
Access Control Language
Lease Schema
Building Permit Certificate Schema
Occupancy Permit Certificate Schema
Property Title Schema
Municipal Charter Schema

The implementation of the legal instruments and real estate methods and procedures in an online environment that the above items represent

A language implementing the method of calculating monthly rent to be paid for the use of an online facility

A System for the Assignment and Management of Responsibilities, Privileges and Access Controls

Facilities Management: The Role Description Language

The Osmio VRD Birth Certificate takes the place of the visual cues that identify who is in a room with us.

In physical space managers can see and hear who is doing what, monitor performance, know whether people have the authority to do what they're doing and intervene where necessary. With online spaces, the facility itself must "understand" and enforce the roles and responsibilities of the space.

The roles must be expressed in a language that is understood by both people and facilities. The following is a list of default titles, access controls, and privileges for a facility. These are defaults; you need not use all of them, and can easily add others.

Titles & Responsibilities

Title	Responsibility
Chief	Everything within a facility where tenant is in good standing
Manager	Anything delegated by Chief
Member in good standing	Participate in any non-restricted activity
Member not in good standing	Participate in activities where blockage (default) has been overridden by Chief or his/her delegate
Administrator	Maintains files made available to membership by management or by other members; may also serve as research librarian and perform other administrative tasks
Property Manager	Services the tenant; ensures that facilities are in good shape; notifies tenants of contract violations; enforces terms of lease
Property Owner	Negotiates leases with tenants; activates lease/tenancy files; revokes tenancy privileges and access to tenant files

Management of access control lists and privilege lists is part of the Building Codes Component. Access management and privilege management are separate; both are role-based. Following are some of the roles in the default access control system of the Building Codes Component:

AccessControl Delegations	Title	May Grant To
All tenant records within this facility	Chief	Manager, Administrator
Member Records	Chief	Manager, Administrator
Lease & rental records	Manager	
Architectural files (facility parameters)	Chief	
Pre-release submissions to Library	Administrator	
Facility software	Chief	
Moderator schedule & privilege files	Manager	
Tenancy financial files	Chief	

Following are some of the roles in the default privilege control system of the Building Codes Component for use within a facility:

Privilege	Title	May delegate to
Create a new facility within this facility	Chief	No one
Assign any privilege	Chief	Manager
Revoke any privilege	Chief	Manager
Edit banners	Manager	Anyone
Manage library	Librarian	Anyone
Moderate any conference	Manager	Anyone
Pick up tab for guest's usage	Chief	Manager
Open a shop for a vendor	Chief	Manager
Manage vendor listings	Manager	Vendor
Manage shopping cart functions	Manager	Marketplace Manager
Notified of Library submissions	Administrator	Anyone
Manage general member access/priv	Chief	Manager
Manage specific member access/priv	Manager	Assistant Manager

Other roles at the property owner or municipality level of the Building Codes Component apply to the permitting of the facility itself:

Privilege	Title	May delegate to
Charter a new community	Chair, Osmio Communities Commission	No one
Edit/recompile facility software	Licensed Architect or Contractor	No one
Issue an occupancy permit	Osmio Chief Building Inspector	Community Building Inspector
Create a new facility	Property Owner	Community Facilities Manager
Issue a lease for a new facility	Property Owner	Community Facilities Manager
Edit/revoke tenancy privileges	Property Owner	Property Manager

While these titles and privileges are role-based, it is not the role that takes the actions but rather the holder of the identity credential that is linked to the role. At every level a formal delegation must be made, binding the Osmio VRD identity credential to the role. A change in roles requires revocation of previous bindings.

A complete description of the Building Codes Component and the Real Estate Markup Language would take much more space than is available here. That's assuming all the work is done, which I assure you is not the case. But enough is done to start building some nice, if simple, facilities.

A community's building codes may permit the use of any client software that enables the use of X.509 certificates. In addition to those codes, a more stringent set of codes will be available for tenants who need a higher level of security than most common client operating systems provide. These codes will specify the use of client operating systems that have passed the Osmium security audit.

Let's take a look at the product that is built upon such a rugged kernel. It is Dorren, the operating system that knows the difference between indoors and outdoors.

To see the current state of development of

The Building Codes Component
…and to learn how your

experience in the architecture
and code compliance professions
might be put to use in its development, please go to the Building
Codes Component Development Office at osmio.ch