

Interagency Advisory Board

Meeting Agenda, December 7, 2009

1. **Opening Remarks**
2. **FICAM Segment Architecture & PIV Issuance** (*Carol Bales, OMB*)
3. **ABA Working Group on Identity** (*Tom Smedinghoff*)
4. **F/ERO Repository** (*Elisa Cruz/FEMA*)
5. **Correlation of SP 800-53 rev. 3/ FIPS 201/ SP 800-63/ PIV-I/ FICAM Segment Architecture** (*Matt Scholl/Bill Macgregor, NIST*)
6. **Use of Optional Form Factor to Meet PIV-I** (*Andrew Sheedy, ActivIdentity*)
7. **Closing Remarks**

ABA Task Force Project Federated Identity Management Legal Issues

**Thomas J. Smedinghoff
Wildman Harrold
Chicago**

Co-Chair, ABA Federated Identity Management Legal Task Force



Agenda

- Overview of the American Bar Association IdM Legal Project
- Some thoughts on Addressing the Legal Issues of Identity Management

American Bar Association Federated Identity Management Legal Task Force

ABA Federated Identity Management Legal Task Force



Wildman Harrold
Attorneys and Counselors

- Established January 2009
- Part of ABA Section of Business Law, Cyberspace Law Committee
- Co-Chairs
 - Thomas J. Smedinghoff, Wildman, Harrold, Allen & Dixon LLP
 - R. David Whitaker, Wells Fargo Bank
 - Jane K. Winn, University of Washington School of Law

ABA Federated Identity Management Legal Task Force



Wildman Harrold
Attorneys and Counselors

- It's an open project. Participants include:
 - Lawyers, non-lawyers, IdM technology experts, businesspersons, and other interested persons
 - From businesses, associations, and government agencies
 - From U.S., Canada, EU, and Australia so far
- Website (and sign up for listserv) at –
 - **www.abanet.org/dch/committee.cfm?com=CL320041**
 - Alt. URL: **<http://tinyurl.com/yft89m8>**
- Next In-person meeting: Miami, January 29-30, 2010

ABA Federated Identity Management Legal Task Force



Wildman Harrold
Attorneys and Counselors

- Goals –
 - Identify and analyze the legal issues that arise in connection with the development, implementation and use of federated identity management systems;
 - Identify and evaluate appropriate legal models to address issues;
 - Develop model terms and contracts that can be used by parties
- Initial efforts
 - Develop common definitions of key terms (from legal perspective)
 - Identify legal issues
 - Identify legal models to address issues
 - Develop model contract language
- We're seeking participants and input –
 - Please join us, and send us your contracts!!

Addressing the Legal Issues



“Liability” Per Se Is Not the Issue

- “Liability” is just the penalty when you (or someone else) does something wrong
- We need to define when something is wrong
 - What are you required to do?
 - What are you prohibited from doing?
 - What are you committing to (e.g., representations)?
 - What standard is applied to your conduct?
- We need to identify the legal issues of concern
 - We can’t address the issue unless we know the potential source of the liability – e.g., warranty, antitrust, tort, contract, duty to authenticate, etc.
 - See, e.g., American Bankers Association CA Liability Analysis (1998), at www.wildman.com/resources/articles-pdf/ca-liability-analysis.pdf

Consider the Sources of the Legal Issues



Wildman Harrold
Attorneys and Counselors

- Statutes and regulations (in all relevant jurisdictions)
- Common law / judicial decisions
- Standards
 - Industry associations (e.g., PCI DSS)
 - System rules – e.g., Visa rules, ATM system rules
- Self-imposed requirements**
 - Unilateral undertakings, such as privacy policy or CPS
- Contracts among the parties**
 - Trust frameworks
 - Bilateral agreements

(** can solve some legal issues and create others)

Consider Factors that Affect the Legal Issues



Wildman Harrold
Attorneys and Counselors

- Nature of the person involved
 - e.g., Individual, consumer, business, corporate entity, government entity
- Expertise of the person involved
 - e.g., professional / in the business, etc.
- Nature of the information involved
 - e.g., sensitivity of personal information (e.g., name vs. SSN)
- Nature of the use involved
 - e.g., login to garden club website vs. launch nuclear missiles
- Nature of any resulting harm
 - e.g., embarrassment, economic losses, property damage, personal injury
- Level of assurance / level of protection involved
- Legal jurisdictions involved
- Interplay of statutes, regulations, standards, and contracts



Consider Categories of Legal Risks

- **Assessment risk**
 - Was IdP (or even assessor/auditor) properly certified?
- **Performance risk**
 - Failure of any participant to perform
- **Technology and security risk**
 - What is something doesn't work properly
- **Identification risk**
 - Risk of incorrect identification, identity theft; failure to satisfy obligation imposed by law
- **Authentication risk**
 - Authentication compromised / identity theft / fails to satisfy obligation imposed by law
- **Privacy risk**
 - Improper or unauthorized collection, use, or disclosure of personal information
- **Compliance risk**
 - What if framework doesn't satisfy with role's legal compliance obligations?
- **Third party risk**
 - What if something bad happens that is no one's fault?



Consider Categories of Law

- Contract law
- Warranty law
- Tort law
 - Negligent performance
 - Negligent misrepresentation
 - Fraudulent misrepresentation
 - Defamation
- Third party beneficiary law
- E-transactions law
- Consumer protection law
- Security law
- Privacy / data protection law
- Identity theft law
- Antitrust law
- Unfair competition law
- False endorsement
- False advertising
- IP law
 - Copyright law
 - Trade secrets law
 - Trademark law
 - Patent law
- Statutory/regulatory law
 - Governing the IdM process
 - Imposing IdM compliance obligations
- Liability for the conduct of others
- Governmental immunity law
- Other



Consider Legal Issues By Role

- Basic roles include –
 - Trust Framework Provider / Assessor / Auditor
 - Subject / Identity Provider / Relying party
 - Victim (non-participant)
- For each role in an IdM system, consider the following:
 - What are the concerns that a participant in that role has re participating in and relying on the IdM system?
 - What are the obligations required of a participant in that role in order to make the IdM system work properly
 - What rights does that role have by law?
 - What other rules are necessary, or should be addressed, for a participant in that role?



Wildman Harrold
Attorneys and Counselors

A few examples, focused on “Obligations” and “Concerns” of each Role

For Trust Framework Providers We Need Rules to . . .



Wildman Harrold
Attorneys and Counselors

- Define the scope of the Trust Framework Provider's obligations to . . .
 - Properly certify Identity Providers
 - Periodically audit Identity Providers
 - Enforce compliance with rules by all participants
- Address concerns about . . .
 - Appropriateness of process for developing/amending contracts
 - Nature and scope of warranties/representations it makes by certifying Identity Providers
 - Avoiding practices with antitrust implications

For Subjects We Need Rules to . . .



Wildman Harrold
Attorneys and Counselors

- Define the scope of the Subject's obligations to . . .
 - Provide accurate information
 - Prevent unauthorized use of token or revoke when necessary
 - Control access, keys, passwords, tokens, etc.
- Address concerns about . . .
 - Performance of the Identity Provider
 - Identity theft
 - Privacy and security of Subject's personal data in possession of both Identity Provider and Relying Party

For Identity Providers We Need Rules to . . .



Wildman Harrold
Attorneys and Counselors

- Define the scope of the IdP's obligations to . . .
 - Comply with policies, practices and procedures
 - Properly identify the Subject
 - Provide accurate identity assertions
 - Provide revocation capability or restrict reuse of token
 - Protect the privacy and security of Subject's personal information
- Address concerns about . . .
 - Defining/limiting scope of assertions
 - Obtaining complete & accurate description of proposed uses
 - Limiting scope of use of tokens to acceptable scenarios
 - Possible forgery of identity assertions or tokens
 - Limiting liability generally

For Relying Parties We Need Rules to . . .



Wildman Harrold
Attorneys and Counselors

- Define scope of the Relying Party's obligations to . . .
 - Validate credential/token before reliance
 - Limit use and reliance on credential/token as appropriate
 - Protect privacy and security of Subject personal data
- Address concerns about . . .
 - Identifying and trusting the Identity Provider
 - Defining the scope and time of the identity assertion
 - Understanding the basis for the assertion
 - Ability to introduce assertion as evidence in court
 - Allocation of risk for incorrect assertions



Addressing/Controlling Legal Issues

- Some legal issues cannot be controlled
 - Law governs – cannot be altered; must comply
- Some legal issues can be controlled
 - Law governs, but can be altered by contract, or
 - No law, so parties can determine by contract or other method
- For some legal issues its unclear whether the issue can be controlled
 - Governing law cannot be altered in some jurisdictions, but can be altered (or doesn't exist) in others
 - E.g., SSN transfer must be encrypted in some jurisdictions, but not regulated in others
 - E.G., Consent to transfer of personal data valid in some jurisdictions, not valid in others

We Need an Underlying Legal Framework



Wildman Harrold
Attorneys and Counselors

- To provide the rules that govern the rights and obligations of the parties in a manner that ensures compliance (e.g., by providing penalties/compensation for non-compliance)
- That addresses and resolves the relevant legal issues
- That provides legal certainty and corresponding trust



Approaches to a Legal Framework Wildman Harrold Attorneys and Counselors

- Legislative/Regulatory framework
 - DigSig law in Utah (now repealed) and Washington
 - EU E-Signature Directive
 - Malaysia law; Egypt law
- Unilateral assertion model
 - E.g., original CPS approach
- Contractual framework models
 - See following slides
- Hybrid framework – most likely



Wildman Harrold
Attorneys and Counselors

Examples of Possible IdM Contract-Based Legal Frameworks

Collaborative Framework



Wildman Harrold
Attorneys and Counselors

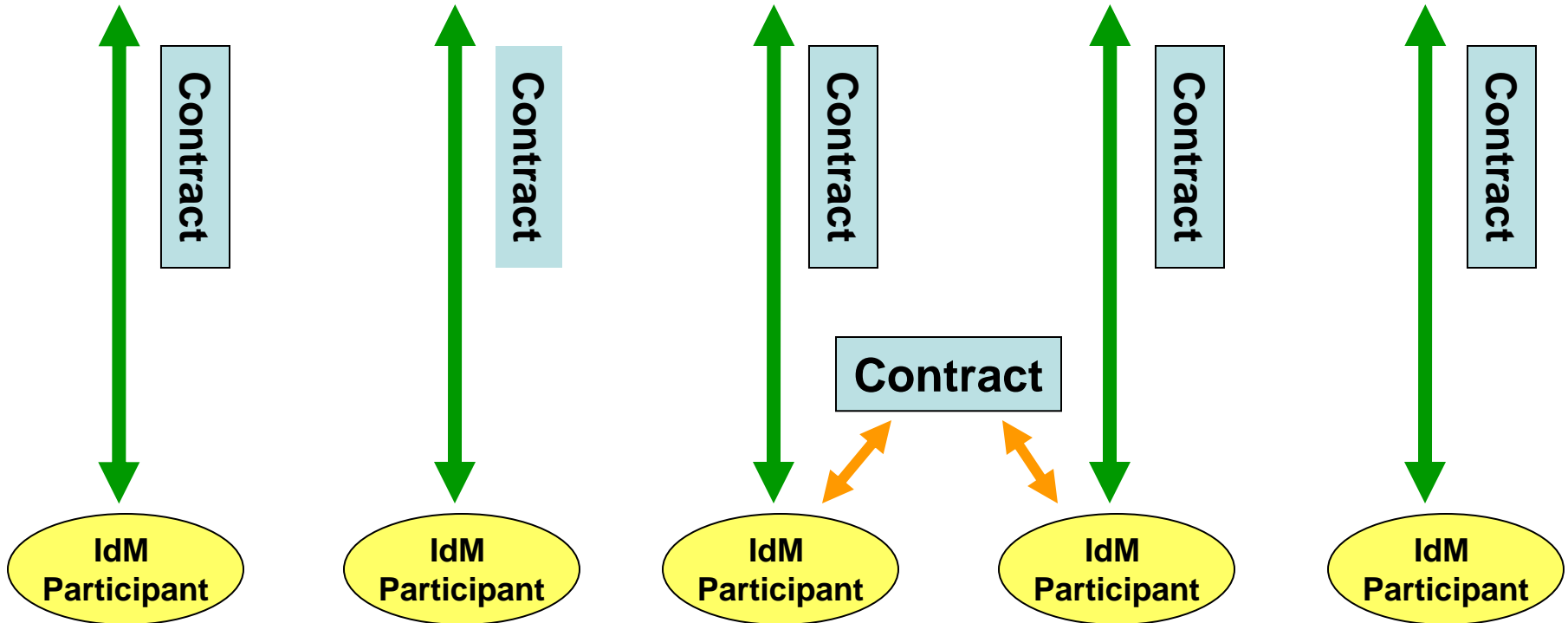
- Group of founders forms an entity that establishes the governance and operating rules
 - All participants (IdMs and RPs) join by entering into contract with entity
 - May also contract with each other too
 - Examples: SAFE-BioPharma, Identrus
- Advantages:
 - Provides single consistent framework and operating authority; useful for large identity federations
- Disadvantages:
 - High startup/operating costs; not appropriate for small identity federations

Collaborative Framework



Wildman Harrold
Attorneys and Counselors

Governing Entity (Formed/Controlled by Participants)



Centralized Framework



Wildman Harrold
Attorneys and Counselors

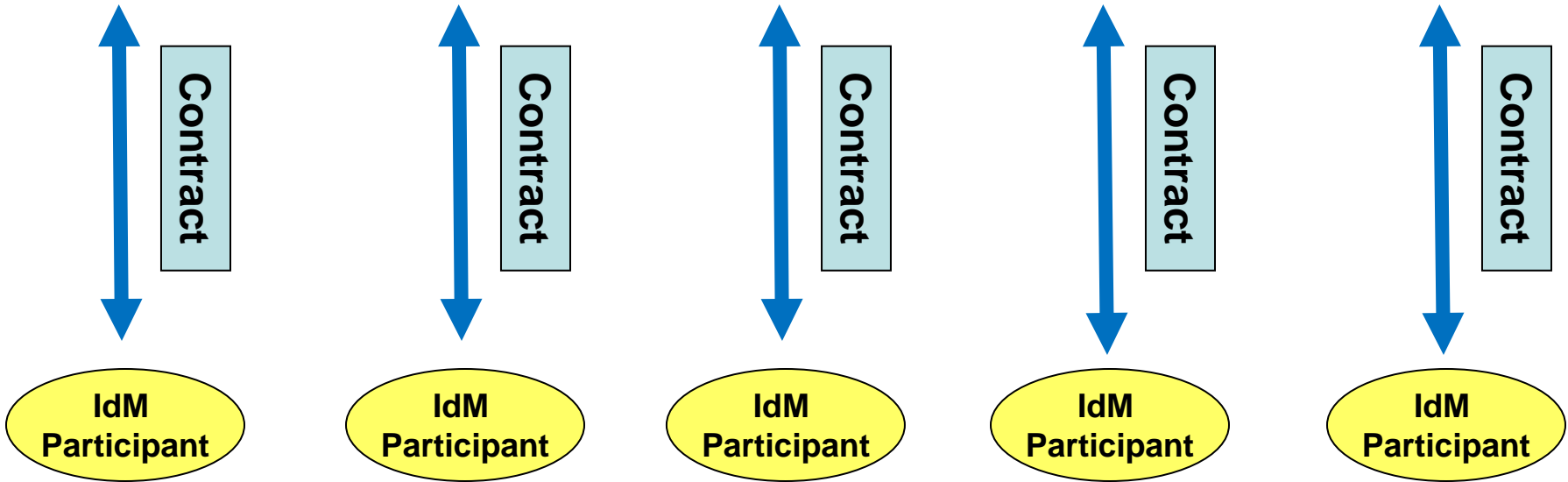
- A single Founder dictates the governance and operating rules for the identity federation
 - Founder enters into contracts with IdM Participants (IdPs and RPs)
 - Example: Federal E-Authentication Partnership; large trading partner scenario (e.g., Wal-Mart)
- Advantages:
 - Useful for identity federations established for benefit of a single party (the founder); provides single consistent framework for benefit of Founder
- Disadvantages:
 - Participants have lesser voice in determining rules / legal obligations; limited purpose application for federation

Centralized Framework



Wildman Harrold
Attorneys and Counselors

Governing Entity
(Founder or Entity Operated/Controlled by Founder)



Consortium Framework



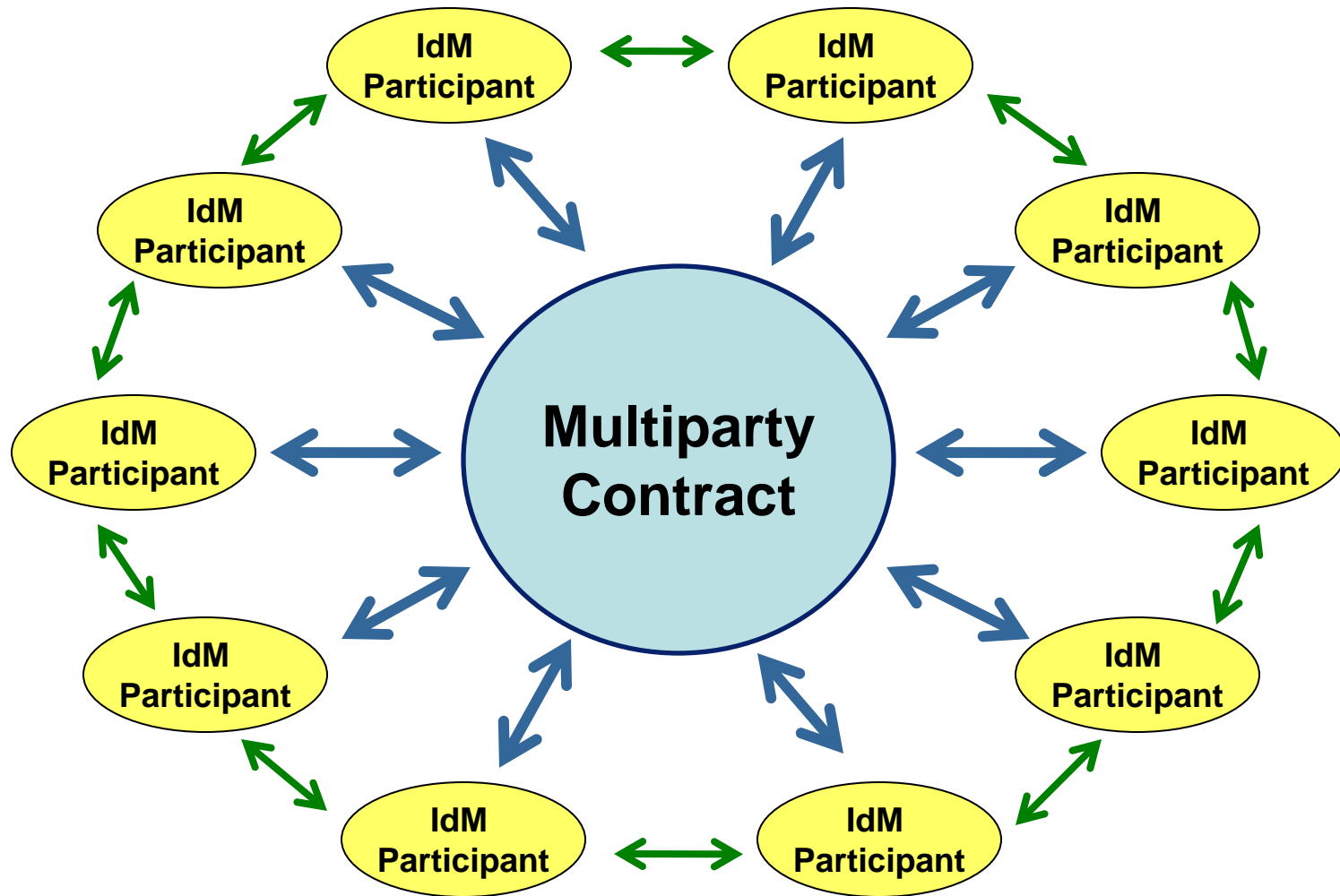
Wildman Harrold
Attorneys and Counselors

- A small number of IdM participants forms a consortium via a multi-party contract that sets the governance and operating rules for the identity federation
 - One contract signed by all participants as parties
- Advantages:
 - Lower costs for small group with stable membership; less formal than Collaborative Framework
- Disadvantages:
 - Cumbersome where participants are in flux; higher ongoing coordination costs; difficult to scale

Consortium Framework



Wildman Harrold
Attorneys and Counselors



Bilateral Framework



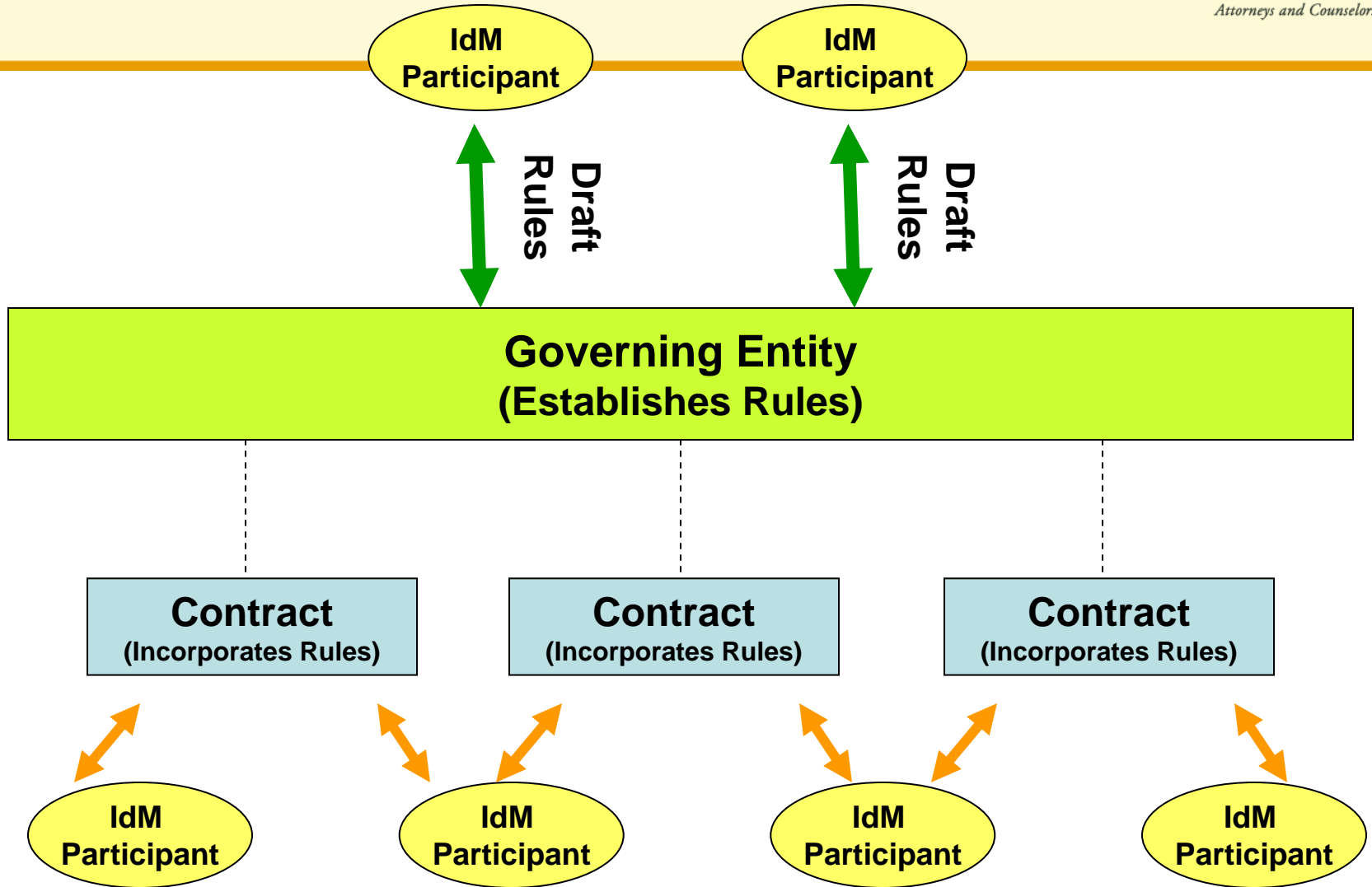
Wildman Harrold
Attorneys and Counselors

- Group of Founders forms a policy entity that establishes the governance and operating rules
 - All participants (IdMs and RPs) contract between themselves with respect to their identity federation activities (NOT with the policy entity)
 - Participants separately negotiate issues such as risk of loss / liability
- IdM participants enter into contracts with each other that incorporate the rules by reference
- Advantages:
 - lower startup costs; easy scalability – anyone can adopt rules in a bilateral contract
- Disadvantages:
 - decentralized responsibility for compliance increases potential for inconsistent application

Bilateral Framework



Wildman Harrold
Attorneys and Counselors



Third Party Assurance Framework



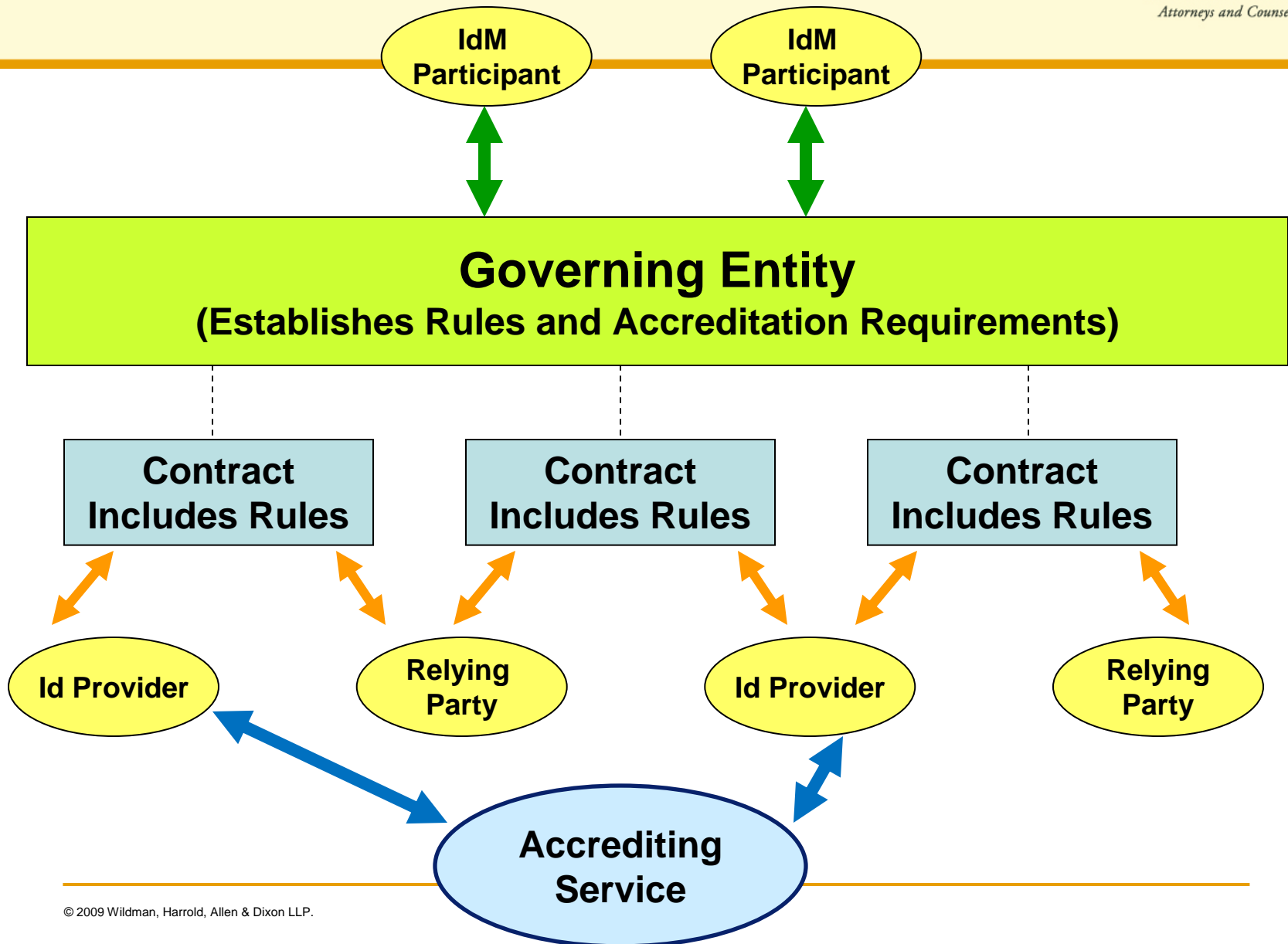
Wildman Harrold
Attorneys and Counselors

- Similar to Bilateral Framework but IdP compliance with governance and operating rules enforced by requirement for third party accreditation and audit
 - Relying Parties and Identity Providers use their existing business contracts much like the Bilateral Framework
 - Relying Party obligates the Identity Provider to obtain the required accreditation and maintain it in good standing
 - Example: CA/Browser Forum for EV SSL Certificates
- Advantages:
 - Combines best of Collaborative Framework and Bilateral Framework; still allows maximum flexibility between bilateral parties; reduces potential for inconsistent quality or application of rules; 3rd party certification reduces compliance monitoring
- Disadvantages:
 - Enforcement is still decentralized; Higher ongoing coordination costs

Third Party Assurance Framework



Wildman Harrold
Attorneys and Counselors



Further Information



Wildman Harrold
Attorneys and Counselors

Thomas J. Smedinghoff

Wildman, Harrold, Allen & Dixon LLP

225 West Wacker Drive

Chicago, Illinois 60606

312-201-2021

smedinghoff@wildman.com