

Trust Starts at Hire

The architecture that connected employment, identity and digital trust, long before autonomous AI.

Raymond Carlson

CARLSON BUSINESS VALUE ENGINEERING™
U.S. COPYRIGHT REG. NO. TXU 2-524-043

Documents of consequence **still moved by courier.**

I came out of the reinvention of HR with the life-event architecture, and with a clear view of what the HR system of record really holds: the enterprise's verified record of who its people are, and of every change in their standing.

Then I stepped into a \$50 million venture-backed service at the frontier of internet commerce. Legal, medical and financial documents still moved by courier, because nothing electronic could carry the trust they required. The service would move them electronically, and it had to prove everything a courier's signature proved, and more. Who sent it and who received it, each authenticated. That no one altered it and no one else saw it. That neither party could later deny its part. And a permanent, high-security record that it was sent, kept for good.

Every one of those guarantees rested on identity. Insurance and financial assurance would attach to each transaction at silver, gold and platinum levels, and each level demanded identity bound more strongly than the last.

THE QUESTION

Where does identity strong enough to insure come from?

The plan sent every user to a certificate authority. **That was the flaw.**

When I walked in, the venture had an answer to identity. Every sender and every recipient would go to VeriSign, the commercial certificate authority, one person at a time, and obtain a digital certificate. The certificate would bind the person to the message.

The plan failed on two counts. The first was scale. A service meant to become as ubiquitous as the courier it replaced needed its users credentialed by the hundreds of millions, and a certificate authority issuing to one person at a time could never get there. The second was assurance. A certificate authority meeting a stranger once, at a distance, cannot establish identity to the standard gold or platinum demands, and nothing it does afterward tells it when that person changes jobs, gains authority or leaves. No insurer would stand behind a transaction on that basis.

I recognized the problem the moment I saw it, because I had just spent years inside its solution. Every employer verifies a person before it hires them, keeps that identity current until the day they leave, and records every change in between in the HR system of record. Bind the certificate to that record, let the employee's life events drive its lifecycle, and identity on the internet inherits the trust the enterprise has already established.

DAY ONE

I drew the architecture the first day: the employer as identity authority, life events as the certificate lifecycle. It was the life-event architecture of HR self-service, carried into digital trust.

The principal investor saw the architecture as the opportunity for the next venture and asked me to lead it. A Big Six professional services firm and a private merchant bank backed the two as sister ventures. The messaging service moved the documents. The second, which I co-founded, would vouch for who people were: a Registration Authority, working alongside a separate commercial Certificate Authority.

THE VENTURE

\$50M

VENTURE-BACKED

3

ASSURANCE LEVELS: SILVER,
GOLD, PLATINUM

4

GUARANTEES:
AUTHENTICATION, INTEGRITY,
NON-REPUDIATION, PERMANENT
RECORD

1

MISSING PIECE: IDENTITY
STRONG ENOUGH TO INSURE

Two authorities, two jobs.

Public-key infrastructure separates two roles, and the whole architecture depends on the difference. One decides whom to trust. The other produces the proof.

FUNCTION	REGISTRATION AUTHORITY	CERTIFICATE AUTHORITY
Verify who the applicant is	Primary responsibility	Relies on the Registration Authority
Validate organizational affiliation and authority	Yes	Relies on the Registration Authority
Approve or reject certificate requests	Yes, under the Certificate Authority's policy	Controls issuance
Generate keys	No	Not necessarily; the applicant usually generates the key pair
Sign and issue the certificate	No	Yes
Lifecycle	Validates changes and requests revocation	Renews, revokes and publishes revocation

THE DIVISION

The Registration Authority establishes whom to trust. The Certificate Authority cryptographically certifies that trust.

In my architecture, the venture was the Registration Authority, turning the employer's existing verification into a registration service. A separate commercial Certificate Authority signed and issued the certificates on the strength of it.

The employer is the identity authority.

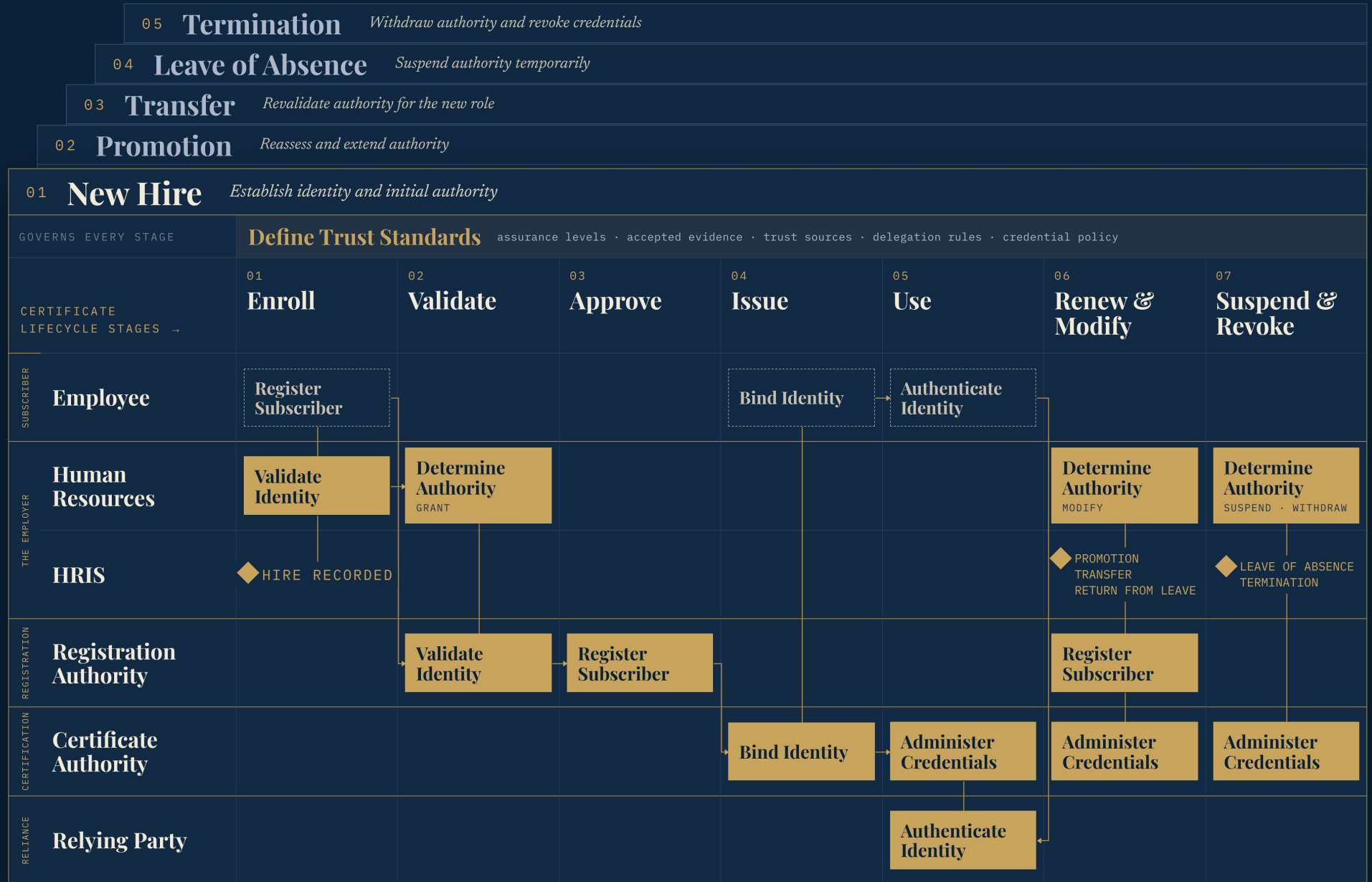
The HR system of record is the authoritative record of who works for the enterprise and in what role. That record is established at hire through verification the employer is already required or motivated to perform: employment eligibility documentation, government identification, and background checks that scale with the seniority and sensitivity of the role. An outside certification authority verifies a person once. The employer verifies them at hire and holds an ongoing relationship with them for as long as they work there.

The same life events that drove HR self-service become the events that govern a digital identity. Each one is an institutional decision first. Issuing, upgrading or revoking the certificate is the consequence.



THE BINDING

Identity on the internet inherits the trust the enterprise has already established, and loses it when the enterprise does.



Identity is verified. Authority is institutionally governed. Credentials establish trusted digital identity within those boundaries.

■ Performs □ Participates

© 2026 Raymond Carlson · Carlson BCM™

Vet the vetter. The chain needed a root.

The employer can vouch for its people only if someone has vouched for the employer. A small family business and one of the largest industrial companies in the country cannot enter the chain on the same terms.

I took the question to the leading business credit bureau, which already assigned a unique identifier to nearly every company in the country. Would it become a Registration Authority itself, and could its registry anchor a proposed trust architecture in which each verified enterprise received a certificate, issued beneath a trusted certification authority, authorizing it to certify its own employees? The bureau would establish that the enterprise was real. The certification authority would remain the cryptographic root.

LAYER	WHO VOUCHES	WHAT IT ESTABLISHES
Enterprise	The business credit bureau's registry	The company is real, and is who it says it is. Under the proposal, it vouches for its own employee chain.
Integration	The registration service	Connectors to the major HR and ERP packages carry life events into the certificate lifecycle.
Employee	The employer, through the HR system of record	The person is verified at hire and certified under the enterprise root.
Lifecycle	Employee life events	Issue, upgrade and revoke follow hire, promotion and termination.

The work exposed the registry. Companies were cataloged without being vetted. Records were not reviewed on any regular cycle, so much of the data was stale. Poor data was the product of poor collection practices. The architecture needed enterprise records verified and maintained more rigorously than the registry supplied, and closing that gap became part of the design.

THE GOVERNING PRINCIPLE

You cannot establish a trustworthy digital identity by cryptographically certifying an untrustworthy physical identity.

The cryptography can be sound while the identity beneath it is not. A root of trust is only as good as the registry beneath it.

Reach the system of record, **wherever it lives.**

A verified enterprise and a sound certificate are not enough. Life events can drive the certificate lifecycle only if the service can read them from the system where they are recorded, and every enterprise records them somewhere different.

Research scientists from one of the country's great industrial laboratories came over to engineer it. They built connectors into the major HR and ERP packages of the day: PeopleSoft, SAP, Oracle and Lawson, with the largest payroll processor a question of feasibility. No set of connectors covers every company, so the service itself became the integration layer: one service working across many enterprise platforms, prioritized by market share, rather than requiring any participant to adopt a particular package.

Years later, I built the same kind of capability for a major life insurer. To control payroll slotting for worksite insurance, the carrier had to integrate with the payroll and ERP systems of every employer it served. Different object, same architecture.

	THE REGISTRATION SERVICE	THE LIFE INSURER
Enterprise problem	Establish trusted corporate and employee identities	Control payroll slotting across employers
External systems	HR and ERP platforms	Payroll and ERP platforms
Requirement	Integrate identity and credential processes	Integrate payroll allocation and deduction processes
Objective	A scalable digital trust service	Worksite insurance distribution at scale

THE ASSET

The certificate was the credential. The verification and integration service was what made that credential commercially useful at scale, for everyone from the enterprise to the ordinary person who needed to be trusted online.

Seven abilities, **one verb each.**

Rebuilt in Carlson BCM grammar, the architecture becomes an addition to the common functional corpus. Level 1 is Common Functional. The substantive model begins at Level 2: seven enterprise capabilities, each verb taken from the Carlson Verb Reference. Life events are triggers that invoke these capabilities. They are not capabilities themselves.

LEVEL 2	WHAT IT DOES
Define Trust Standards	Sets the rules: assurance levels, evidence, authentication strength, accepted trust sources, delegation rules, credential policy. The only capability that sets rules rather than applying them.
Validate Identity	Decides whether a claimed identity is true, for a person, an organization or a non-person entity, and whether a trust source can be relied on.
Authenticate Identity	Confirms, each time an identity is used, that the right party is using it.
Determine Authority	Decides what any entity in the trust hierarchy may do, including delegated authority and the effect of a life event on authority.
Register Subscriber	Admits a validated entity to the trust framework, holds that relationship, and decides whether its standing warrants a credential. The Registration Authority's ability.
Bind Identity	Binds a validated identity to a credential that relying parties can verify independently. The Certificate Authority's ability.
Administer Credentials	Governs a credential's standing once it exists: renewal, suspension, reinstatement, termination, and making that status known.

Beneath them sit 42 candidate Level 3 business capabilities. The one that carries the invention is the ability to determine a change in authority, under Determine Authority. Each Level 3 states what the enterprise can do, never how. Life events are attributed to it as triggers, and that attribution is the employer-lifecycle binding.

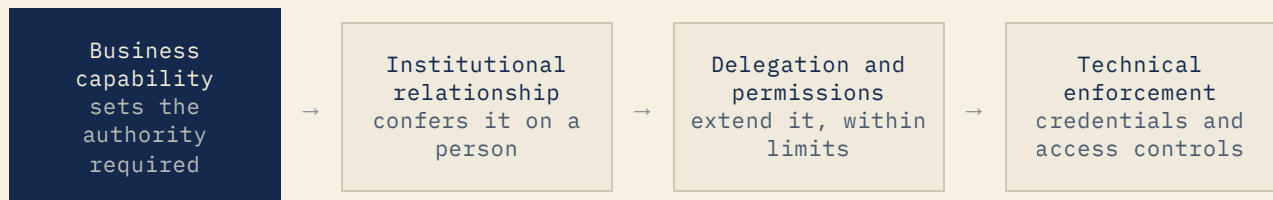
PRINCIPLE DEMONSTRATED

Carlson BCM grammar does not merely standardize how capabilities are written. It exposes whether the architect has understood the ability being described.

Identity says who. Authority says what it may do.

Identity and authority are capabilities of the enterprise, bound to the events that change them. The architecture kept them apart on purpose. Validating who someone is answers one question. Determining what they may do answers another, and the answer changes every time the relationship beneath it changes.

An employee holding a valid certificate is promoted, transferred or terminated. The identity has not changed. The authority has. A credential can remain technically valid after its basis is gone, and that is exactly the separation the architecture formalized.



Least privilege is a constraint on authority. It is not the source of authority. Technical enforcement can constrain what an entity does. It cannot, by itself, establish whether that entity was legitimately authorized to do it. The capability sets the authority required. The institutional relationship confers it on whoever performs the work. Life events change or end that relationship, and every link after it must follow.

THE DISTINCTION

A change in authority is a decision. Its effect on the credential follows from it, never the other way round.

The Agent Has a Credential. Who Vouched for Its Authority?

Then, the question was whether the internet could trust an employee acting for a company. Now, it is whether an enterprise can trust an agent acting for that employee. The seven capabilities read straight across.

LEVEL 2

IN THE AGENTIC ENTERPRISE

Define Trust Standards	What evidence, authentication strength and delegation limits must an agent meet before it is trusted at all?
Validate Identity	Which agent is this, and who built it and deployed it?
Authenticate Identity	Is the agent calling this system really that agent?
Determine Authority	What may it do, and whose authority is it acting on?
Register Subscriber	Who admits an agent into the enterprise, and on what evidence?
Bind Identity	Binding the agent to a credential other systems can verify.
Administer Credentials	Suspending or revoking it when its owner leaves or its mandate ends.

Delegated authority runs through a chain: enterprise to authorized person to agent to action. Each link needs a legitimate basis, and each must stay valid when the relationship beneath it changes. A sponsor's termination, transfer or promotion changes the agent's authority, and the agent has life events of its own: deployment, reassignment, suspension, replacement, retirement. An agent still running after its owner has left is the certificate nobody revoked.

01

Vet the vetter

An agent registry is only as good as its checks on what it registers.

02

The employer as the authority

A vendor can attest to what the agent is. Only the enterprise can grant it authority to act.

03

Registration apart from certification

Deciding whom to trust stays separate from producing the proof.

An agent's intelligence does not establish its legitimacy.

carlsonbcm.com/engagements/trust-starts-at-hire

© 2026 Raymond Carlson · Carlson Business Value Engineering™

U.S. Copyright Registration No. TXu 2-524-043 · All rights reserved.